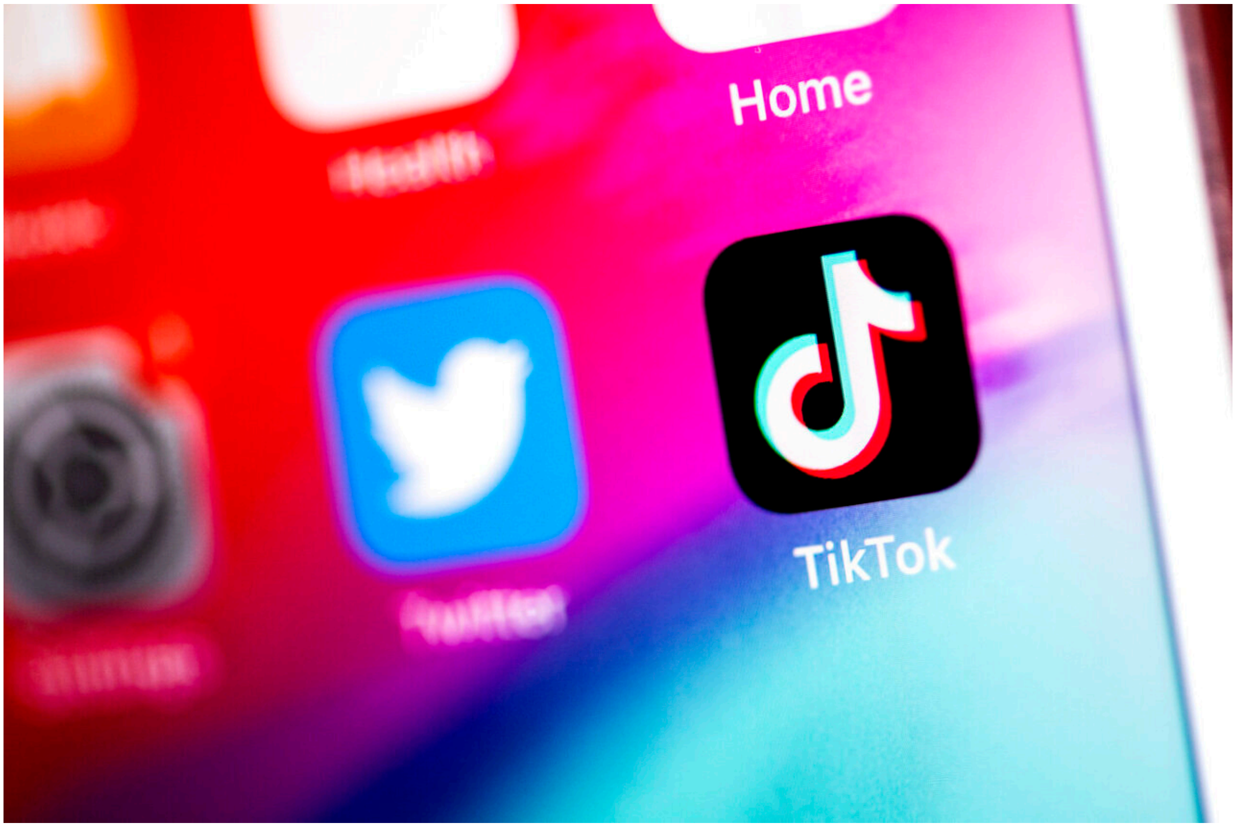
Does TikTok pose data espionage concerns for the US? The answer is complicated

June 15 2022, by Jackson Cote



Credit: Ruby Wallau/Northeastern University

While Chinese-owned social media platform TikTok has had a meteoric rise in popularity since it was released in 2016, the app's growth has posed privacy concerns when it comes to the collection of users' information, highlighting what a recent New York Times op-ed labeled a "data espionage problem."

The fear surrounding so-called data espionage is that social media apps collect users' data in vast quantities, which can be used by adversarial governments for harmful purposes. TikTok is owned by the Chinese company ByteDance, and some cybersecurity experts warn that the authoritarian country, which already monitors its own citizens through different emerging technologies, could use the platform to gather and exploit consumers' information.

"TikTok has this unique position in that it's very popular and getting more popular, but it has this weird ownership structure," says Northeastern computer science professor Christo Wilson, a founding member of the university's Cybersecurity and Privacy Institute. "Anything you see on that platform or interact with or generate, they see that. Like many mobile apps, it has a lot of different, sensitive information that it's collecting, and that's getting shipped off to China."

Last year, President Joe Biden ordered the federal government to review security concerns posed by TikTok and related apps, Reuters reported. And last month, the Senate passed a bill to ban federal employees from accessing the app on government mobile devices, while the U.S. Army and Navy have issued similar bans.

A big question has arisen in light of these cybersecurity concerns, notes Dr. Meryl Alper, a professor of communication studies at Northeastern: How much of a relationship does ByteDance have with TikTok? The answer to this inquiry could determine how much influence the Chinese Communist Party has on the operations of the app in the U.S.

"It's really unclear the role of the Chinese government in terms of who's reporting to who and how independent is TikTok from the rest of

ByteDance," says Alper, who researches the social and cultural implications of communication technologies. "That's something that's very unclear."

There is little evidence, she notes, that the Chinese government has been influencing content available on TikTok in the U.S. However, China has—through its version of the app, Douyin—censored information on domestic issues sensitive to the Chinese Communist Party, like Tibetan independence and the internment of hundreds of thousands of Uighurs, the predominantly Muslim ethnic group in the country.

Another pushback to concerns surrounding data collection by TikTok in the United States is the fact that other apps have been collecting and selling consumers' information for years, Wilson points out.

"There are many other apps that are collecting more or similar information, and they're selling it relatively inexpensively," he says. "I don't think TikTok or China are unique in that respect. We have very weak data privacy laws in the U.S. There's just this data free-for-all going on."

Part of what has driven data privacy concerns about TikTok in the United States is what Alper describes as "personal politics" carried over from former President Donald Trump's time in office. It is no secret, she notes, that Biden's order last year came on the heels of the Trump administration's adversarial relationship with TikTok, which was partially based on the perception that the app fomented youth activism critical of the former president.

"There's a legacy here that is rooted in, yes, valid concerns about national security, but the entire thing is tinged with personal politics that has sort of landed in the Biden administration," Alper says.

Alper points out that cybersecurity concerns have cropped up not just with TikTok, but also with domestic social media giants. Facebook, for example, was manipulated by Russian agents in the lead-up to the 2016 election to sow discord among Americans, she notes.

"While the threat of TikTok to U.S. national security remains theoretical, the threat of Twitter and Facebook is well-documented, especially as it relates to domestic terror," she says.

These dangers, both potential and realized, have led to a larger debate on how information should move globally, according to John P. Wihbey, Northeastern professor of media, innovation and technology, whose research focuses in part on policy issues related to social media platforms.

"There's a very broad reconsideration of how data-flows go across borders, the idea of data sovereignty and the ability to control what's in one's national borders. It's a big policy conversation," Wihbey explains.

According to Wihbey, another discussion is simultaneously underway in American government, academia, and industry: a strategic conversation focused on China. In the past two decades, the nation has become more of an adversary to the United States, and more recently, it has been developing the next generation of artificial intelligence software and surveillance.

"We used to talk about promoting partnerships with Beijing. Now, we're talking about China as a competitor, particularly in the world of technology and AI," Wihbey says. "Some of these concerns can be overblown, but this is a new era of competition between these two countries."

What specific dangers information exploitation can lead to is a "tricky question," as it is all a matter of what kind of data is available, Wihbey explains. What type of information is being collected can determine the resulting threat, he notes.

"With corporations, there are issues of strategic competition implicated there," Wihbey says. "Would data collection allow you some sort of hacking or espionage advantage? Possibly. This could potentially lead to the loss of intellectual property or access to government officials."

These potential dangers show a need for better user privacy safeguards, because regulations that protect people's personal data from technology companies are sorely lacking, Alper, Wilson and Wihbey all point out.

"Our bigger platforms need greater fiduciary responsibilities that are written into law," Wihbey says. "We need more protections for user data and how it's monitored and collected."

"We cannot rely on companies to self-regulate themselves," Alper adds. "That has literally not worked for any industry."

Provided by Northeastern University

Citation: Does TikTok pose data espionage concerns for the US? The answer is complicated (2022, June 15) retrieved 26 April 2024 from https://techxplore.com/news/2022-06-tiktok-pose-espionage-complicated.html