

Trump Might Ban TikTok. Here's What Experts Who Pored Through Its Code and Privacy Policies Say About Its Security.

July 10, 2020 7 min read

This story originally appeared on Business Insider

TikTok, the video-sharing app whose meteoric rise amongst teenage users has made it a challenger to the likes of Facebook, is under attack thanks to its Chinese roots.

The Trump administration said this month it's considering banning the app in the US altogether.

Secretary of State Mike Pompeo first broke the news on Monday, telling Fox News' Laura Ingraham the administration was considering a ban on national security grounds.

Pompeo warned viewers that downloading the app could mean their data ends up "in the hands of the Chinese Communist Party."

Related: U.S. Government Considers Banning Tik Tok

And online gaming megastar Tyler "Ninja" Blevins on Thursday announced he was deleting the app over privacy concerns.

"Hopefully a less intrusive company (data farming) that isn't owned by China can recreate the concept legally," Blevins tweeted. Blevins is not a politician, but is followed by millions of young people – TikTok's biggest demographic – who hang on to his every word.

TikTok is owned by Chinese tech giant ByteDance, which is headquartered in Beijing.

The argument put forward by the Trump administration is that TikTok hoovers up vast amounts of user data which the US then fears could be used by the Chinese government.

That 'Chinese spying' message has not been entirely consistent, as Trump has also suggested a ban could be put in place as a way to punish China for the coronavirus.

But is TikTok actually any worse for snooping in your personal data than social media platforms like Facebook and Google? Business Insider spoke to privacy experts to try to get an answer.

In terms of the data TikTok says it sucks up, it doesn't appear to be worse than Facebook

Zoé Vilain, chief privacy and strategy officer at privacy app Jumbo told Business Insider that looking at TikTok's privacy policy, it was no more intrusive than Facebook's.

"From what I see from the privacy policy, and in comparison with the privacy policies of Facebook and Instagram, I don't really see much difference.

Related: How to Use TikTok to Promote Your Business

"Basically they are saying that they are using your usage data, behavior data, preferences, friends, contacts, to provide you with their service, to customize the service, and of course to do targeted advertising [...] this is exactly what Facebook is doing and Instagram is doing too," said Vilian.

Mike Pompeo told Fox News the US was considering a ban on TikTok.

Image credit: Laszlo Balogh/Getty images

Vilain pointed out that the main difference between TikTok and Facebook or Instagram is in the kind of data users are routinely plugging into the app, as TikTok relies on video. "I think the main difference is that people are recording themselves and this is being recorded," she said.

There's also the fact TikTok is popular with younger folks.

"Also it's mainly used by teenagers, who are maybe less aware and less concerned about what they are sharing," Vilain said.

The FTC fined TikTok \$5.7 million in February 2019 for inadequately protecting the privacy of its underage users, and on July 7 the agency announced it was looking into allegations that the company continues to violate children's privacy on the app.

There are still "legitimate concerns" around TikTok's lackluster security

Business Insider spoke to iOS developer Talal Haj Bakry, who in March along with developer Tommy Mysk discovered a security flaw in TikTok which meant it was able to access iPhone users' clipboards without their permission, essentially meaning TikTok could read any text the user has copied. The researchers noted that this could be as mundane as a shopping list or more serious data like passwords or financial information.

Subsequently LinkedIn and Reddit's apps were also discovered to be reading iOS users' clipboards, and all three companies have now altered their code after Apple started cracking down on the practice with its iOS 14 update.

A TikTok spokesperson said the reason the app was reading clipboards was to identify "repetitive, spammy behavior," and the company has submitted an update to the App Store getting rid of this feature.

In April Bakry and Mysk also discovered a vulnerability in TikTok which meant users' uploaded videos could be intercepted and even replaced.

This vulnerability was the result of TikTok using insecure HTTP connections to download videos from its servers. "All other social media apps have long made the switch to secure HTTPS for all network connections, in effort to protect user privacy and data integrity.

"Such a basic security failing does not inspire confidence in TikTok's ability in protecting their users' data, and exposes a lax attitude towards security," Bakry said.

Related: Latest TikTok News & Topics

A TikTok spokesperson told Business Insider: "TikTok prioritizes user data security and already uses HTTPS across several regions, as we work to phase it in across all of the markets where we operate."

Bakry thinks TikTok's Chinese roots could be part of the reason it's playing catch-up on security.

"What makes TikTok stand out are the differing data privacy laws and security standards between China and other parts of the world. In the US and Europe, there are various laws and regulations in place to protect end-user privacy," Bakry said. "China is only recently catching up in creating data privacy

laws, but it remains to be seen how effective these new laws will be when put in practice.”

Bakry said there are “definitely legitimate concerns” around TikTok’s security. “Whether it’s intentional or merely the result of move-fast-and-break-things, the inadequate security of social media apps can pose a serious threat. These apps collect massive amounts of data from their users, and they become prime targets for bad actors seeking to steal information,” he said.

Vilain agreed that regardless of whether the vulnerability was left open as a backdoor or the result of shoddy security. “Whatever the reason for this, if you’re not securing the collection of data of course it’s a threat and it’s a violation of the GDPR for example in the European Union, and they should do something about this,” she said.

TikTok has tried to distance itself from its Chinese roots

Regardless of whether TikTok’s app is technically more invasive or insecure than any other social media app, the Trump administration’s argument hinges on the idea that private companies in China can be turned into proxies for the Chinese government.

As scrutiny around the app has built up, TikTok company has desperately tried to shake off the idea that it’s a Chinese company.

“TikTok is led by an American CEO, with hundreds of employees and key leaders across safety, security, product, and public policy here in the US. We have no higher priority than promoting a safe and secure app experience for our users. We have never provided user data to the Chinese government, nor would we do so if asked,” a TikTok spokesperson told Business

Insider.

TikTok itself isn't present in China, but is the international twin of its sister app Douyin, which operates in China.

TikTok has always maintained it doesn't store any user data on Chinese servers, although this was contested in a December 2019 lawsuit filed by a user.

A TikTok spokesperson told Business Insider the app's data is stored on servers in the US with backups in Singapore.

In May 2020 the company hired a new American CEO called Kevin Mayer, formerly a Disney streaming executive.

In July, TikTok announced it was withdrawing operations from Hong Kong alongside a slew of US tech companies following the implementation of China's sweeping new national security laws in the region.

Some critics said the withdrawal smacked of a PR move, given that sister app Douyin is more popular in Hong Kong than TikTok.

On Thursday The Wall Street Journal reported ByteDance is holding talks about shaking up its corporate structure even more to try to help TikTok escape regulatory scrutiny abroad.

<https://www.entrepreneur.com/article/353109>