Why was TikTok banned on Australian government devices? An expert on why the security concerns make sense

April 4 2023, by David Tuffley

Credit: AI-generated image (disclaimer)

Australia has joined a raft of other countries in banning the popular video sharing app TikTok from government devices, as several outlets have today reported.

The move comes after a seven month-long review instigated by Home Affairs Minister Clare O'Neil into security risks posed by social media platforms.

Last week, TikTok CEO Shou Zi Chew was grilled by US politicians in a more than five hour-long Congress hearing. Questions mainly focused on TikTok's handling of user data and whether it could be accessed by the Chinese Communist Party, as well as how harmful content (such as content on self-harm and eating disorders) spreads on the app.

TikTok has maintained user data are stored securely and held privately, with CEO Shou Zi Chew telling Congress: "Let me state this unequivocally: ByteDance is not an agent of China or any other country."

But the evidence seems to suggest a ban was a long time coming.

Some background

Since it was acquired by Chinese company ByteDance in 2017, TikTok (formerly Musical.ly) has faced persistent rumors regarding its handling of user data and privacy.

Despite its assurances, TikTok's privacy policy allows for user data, including browsing history, location and biometric identifiers to be collected and shared with "business partners, other companies in the same group as TikTok, content moderation services, measurement providers, advertisers, and analytics providers."

More worrying is this provision: "Where and when required by law, we will share your information with law enforcement agencies or regulators, and with third parties pursuant to a legally binding court order."

"Where and when required by law" would include the provisions of

China's National Intelligence Law, which came into effect in 2017. It obliges organizations to cooperate with state intelligence agencies, and would oblige Bytedance to share TikTok data from Australia that may be deemed relevant to national security.

ByteDance has tried to distance itself from the perception that it is a Chinese company. According to TikTok's vice president of policy in Europe, Theo Bertram, 60% of ByteDance is owned by global investors, 20% by employees and 20% by the founders.

But it hasn't been enough to dispel fears. In 2020, India was among the first countries to impose a lasting nationwide ban on TikTok (and dozens of other Chinese apps), citing privacy and security concerns.

In December 2022, Taiwan imposed a public sector ban after the US Federal Bureau of Investigation warned the app posed a national security risk. That same month, the US House of Representatives issued a ban on devices used by members and staffers.

More recently, lawmakers of the European Union were banned from having TikTok on their devices.

A host of other countries have also enacted bans, including Canada, Latvia, Denmark, Belgium, the UK, New Zealand, France, Netherlands and Norway.

What are Australia's concerns?

Australia and its allies are engaged in a so-called gray zone conflict with China; this is where TikTok becomes a major concern.

Gray zone conflict can be understood as competition between states and non-state actors that resides in a blurred reality between peace and war.

It involves the strategic use of disinformation, propaganda, economic coercion, cyberattacks, and other forms of non-kinetic (subtle and non-coercive) action.

The danger TikTok poses to Australia is that the means would exist for foreign intelligence agencies to track the location of government officials, build dossiers of personal information, and conduct espionage.

An in-depth analysis of TikTok's software code by Australian cybersecurity firm Internet 2.0 makes for interesting, if not alarming, reading.

The firm determined TikTok requests almost complete access to a user's smart device while the app is active. These data include their calendar, contact lists and photos. If the user denies access, the app keeps asking every few hours until access is granted.

Co-founder Robert Potter told the ABC: "When we did that [pulled apart the code], we saw the permission layer that the phone was requesting was significantly more than what they said they were doing publicly. When the app is in use, it has the ability to scan the entire hard drive, access the contact lists, as well as see all other apps that have been installed on the device."

Potter points out these permissions are "significantly more" than what a social media site actually needs to access.

This isn't an isolated incident. Last year, Buzzfeed released leaked audio from more than 80 internal US TikTok meetings that raised the alarm. According to the Buzzfeed report, China-based employees of ByteDance had repeatedly accessed non-public data about US TikTok users.

In one September 2021 meeting, a senior US-based TikTok manager

referred to a Beijing-based engineer as a "master admin" who "has access to everything." A US-based staffer in the Trust and Safety Department was also heard saying "everything is seen in China."

The tapes overwhelmingly contradict TikTok's repeated insistence about the privacy of user data.

The larger context

Australia's ban on TikTok on government phones is hardly surprising. A partial ban has existed for some time.

The decision speaks to the larger issue of balancing national security interests against the trade relationship with our largest trading partner. The TikTok ban is just the latest manifestation of this struggle.

In 2018, Australia's decision to exclude Huawei from installing its 5G network was based on advice from the Australian Signals Directorate that this would give the Chinese government the means, in time of war, to paralyze the nation's 5G-enabled critical infrastructure. A number of other countries came to a similar conclusion.

China is a nation that takes the long view when it comes to geopolitical strategy. Its planning horizon extends to many decades, and even centuries.

Against a backdrop of escalating gray zone conflict, TikTok is an example of a potentially weaponized tool in China's cyber arsenal that could harvest massive amounts of data for nefarious means. And it's likely not the last of such tools we'll face.

The wisest course of action for Australia would be to also develop a long-term orientation, making plans that reach forward many decades—and

not as far as the next election cycle.

Provided by The Conversation

Citation: Why was TikTok banned on Australian government devices? An expert on why the security concerns make sense (2023, April 4) retrieved 12 August 2024 from https://techxplore.com/news/2023-04-tiktok-australian-devices-expert.html