

WILL: New report explains the national danger posed by the social media app TikTok

Posted on Thursday, Dec 22, 2022

>> **WisPolitics is now on the State Affairs network. Get custom keyword notifications, bill tracking and all WisPolitics content. [Get the app or access via desktop.](#)**

The News: The Wisconsin Institute for Law & Liberty (WILL) issued a new policy report, [The Mysterious TikTok-ing Noise](#). The report recaps the meteoric rise of the China-based social media app “TikTok,” and recounts the invasive ways that the software records data from its users. The report strongly recommends that Wisconsin take heed of federal warnings and follow some other states’ practices in prohibiting the app from government-owned devices.

The Quotes: WILL Senior Research Analyst, Noah Diekemper, stated, “TikTok poses a substantial security risk to state and local governments. Our state government owes it to Wisconsinites to keep public operations safe from technological vulnerability at the hands of authoritarian adversaries.”

“TikTok is Chinese Communist Party spyware and belongs nowhere near government devices,” said Representative Mike Gallagher, Chairman of the Select Committee on China in the U.S. House of Representatives and congressional representative for Wisconsin’s 8th District. “WILL’s report clearly defines the threat it poses to government employees and should leave every Wisconsinite asking one question: Why does Governor Evers continue to allow this app to be on state government devices?”

Background: The Beijing-headquartered app TikTok has become one of the most popular social media platforms in America. But, there are significant concerns about the extent of the software’s reach and concerns that the communist Chinese government could have the ability to access TikTok’s data on U.S. citizens.

Key Findings: TikTok has incredible access to individuals' private data. The app is up-front about some of its data collection, including file names and biometric identifiers like faceprint and voiceprints.

Independent analyses have also found that TikTok helps itself to even more data: not only does it access a phone's photos and contact list, but it has JavaScript that enables it to log individual keystrokes made by the user when browsing online—meaning, it could have access to credit card numbers and passwords. Moreover, materials leaked from TikTok's parent company show that the company is not forthright about how it manages security and users' data, with private U.S. data routinely being accessed by employees in China.

This means that TikTok's statements on the subject should not be taken at face value.

Policy Recommendations: This [report](#) highlights how TikTok poses a national security threat to the personal lives and private information of Americans. In a government context, these vulnerabilities could be catastrophic. Based off of the findings of this report, WILL recommends that Wisconsin's policymakers ban TikTok on all state devices. Wisconsin should join the rapidly-growing number of states that have banned TikTok from government-owned devices. Government employees should also be prohibited from using this social media on state networks or during official working hours.

Read More: [The Mysterious TikTok-ing Noise](#), December 22, 2022