U.S. Rep. Gallagher: Reacts to WILL report: how can Gov. Evers still allow TikTok on government devices?

Posted on Thursday, Dec 22, 2022

WASHINGTON, D.C. – Rep. Mike Gallagher (R-WI) today applauded the work of The Wisconsin Institute for Law & Liberty (WILL) in their new policy report, "The Mysterious TikTok-ing Noise." The report recaps the meteoric rise of the China Communist Party (CCP) controlled app, TikTok, and recounts the invasive ways that the software records data from its users. The report also strongly recommends that Wisconsin take heed of federal warnings and follow other states' practices in prohibiting the app from government-owned devices.

"TikTok is Chinese Communist Party spyware and belongs nowhere near government devices," **said Rep. Gallagher.** *"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?"*

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.*"

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 Chinese Communist Party (CCP) has the ability to access TikTok's data on U.S. citizens, including keystrokes and location.

Key Findings of the Report: 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.

The Report's 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 the full report HERE.