U.S. House of Representatives
CAO
CHIEF ADMINISTRATIVE OFFICER

TikTok Cyber Advisory

While the use of official House-affiliated social media accounts is governed by the individual Office and House rules, we do encourage following best practices that are prudent for anyone using social media platforms. We have published more information on social media best practices on HouseNet at:

https://housenet.house.gov/technology/policies-and-standards/social-media-guidelines

TikTok is a Chinese-owned company, and any use of this platform should be done with that in mind. The "TikTok" mobile application has been deemed by the CAO Office of CyberSecurity to be a high-risk to users due to its lack of transparency in how it protects customer data, its requirement of excessive permissions, and the potential security risks involved with its use. Additionally, we believe the user base should be aware that this application is known to store users' Data Location, Photos, and other Personally Identifiable Information (PII) in servers located in China and potentially mined for commercial and private purposes.

TikTok actively harvests content for identifiable data. TikTok "may collect biometric identifiers and biometric information as defined under US laws," including "faceprints" and "voiceprints," from videos users upload to their platform.

TikTok policy has stated that it automatically collects information about users' devices, including location data based on your SIM card and IP addresses and GPS, your use of TikTok itself and all the content you create or upload, the data you send in messages on its app, metadata from the content you upload, cookies, the app and file names on your device, battery state and even your keystroke patterns and rhythms, among other things.

Security researchers have identified several significant concerns with the TikTok applications, including:

- **Device mapping** - gathers all apps installed on the phone and retrieves other running applications on the phone
- **Location** - device location is checked every hour
- **Calendar** - ongoing access

- **Contacts** - TikTok continually requests access to contacts until given
- **External storage** - App requests external storage and retrieves everything in external storage folder
- **Images** - TikTok saves images in photo album

TikTok may also be able to obtain the following device data:

- Wi-Fi network name
- Past Wi-Finetworks
- Device serial number
- SIM card serial number
- Device ID
- Device MAC address
- Device phone number
- Device voicemail number
- GPS status information
- Subscription information
- Accounts on device
- Clipboard access (often used by password managers)

To reiterate, we do not recommend the download or use of this application due to these security and privacy concerns.

Additional References:

Military services have banned the use of TikTok from government devices:
https://www.nytimes.com/2020/01/04/us/tiktok-pentagon-military-ban.html