Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

July 29, 2020

Sundar Pichai
CEO
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Mr. Pichai:

We write to you regarding Google's application (app) store and the policies you have in place to ensure apps are appropriately vetted, particularly those with close ties to China and the Chinese Communist Party (CCP). As you know, we have been engaged in oversight to ensure a safe and secure experience for all users online. As we deal with the ongoing COVID-19 pandemic, the growth of smart device use and reliance on teleconferencing has only increased our dependence on apps, and with that an additional layer of protection that virtual private networks (VPNs) can provide.

As with any crisis, there are those that seek to exploit opportunities for their own malicious intent. We believe that bad actors may be taking advantage of the American people's trust in your brand, which likely extends to apps available through your store. While we want an open and transparent marketplace that does not limit innovators outside your company, we know there are those that seek to use apps as a means to push through pop-up ads or hijack devices to make it a tool for eavesdropping.

The level of permissions that these apps require may include access to camera, microphone, and contacts, as well as functionality to load other malware for bad actors to control a device even after the original app has been removed. This is especially alarming when it comes from companies with direct or indirect links to the CCP.

It is even more alarming as this relates to the private sector and our committee's jurisdiction over critical infrastructure, including the telecommunications, health, and energy sectors. Employees in these sectors could become targets of such app-driven malware as they work from home. We appreciate the joint public-private sector efforts to address these concerns, but your company must do more to screen such apps so that consumers are not reliant just on news articles to bring this to the attention of policymakers.

Especially alarming are those apps marketed as VPNs, which may create a man-in-the-middle vulnerability and a virtual pipeline for our adversaries to our critical data. This was highlighted in a piece in Forbes earlier this year.[1] We are pleased that companies act quickly when questionable activities are raised on companies like Shenzhen Hawk, which is a subsidiary of Chinese conglomerate TCL, that is partially state-owned. However, it also raises questions on the level of scrutiny that these apps receive when they are admitted to your app store.

Accordingly, please provide written answers and any related documentation to the following questions no later than August 12, 2020:
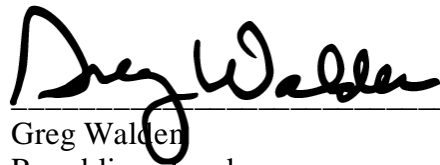
1. Given the reported close ties between TikTok's parent company – ByteDance – and the CCP, do you apply additional scrutiny to the app, including regular audits to ensure the app is in compliance with your policies?

   a. If yes, please detail the additional scrutiny TikTok undergoes.

   b. If no, please explain why not given the national security concerns at play.

2. Please detail your policies as they relate to admittance on your apps store, including what factors are considered to determine if an app meets your data privacy and security standards.

3. Do you proactively audit apps to ensure they comply with your policies or only if a user flags a concern?

   a. If yes, how often do you audit apps on your app store?

   b. If no, why not?

4. If you determine an app is in violation of your policies, what steps do you take to address such violation?

5. Do you maintain a list of app developers who have abused user information or otherwise violated your policies to ensure such developers will not be allowed back on your platform?

---

[1] https://www.forbes.com/sites/zakdoffman/2020/02/24/android-very-dangerous-app-warning-105-million-of-you-have-these-10-threats-on-your-phones/#74c2b3a3a995
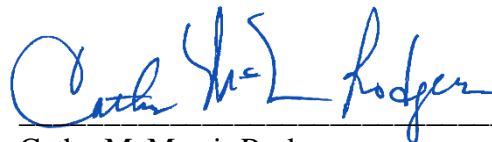
       a. If yes, please explain.

       b. If no, why not?

6. Do you review each app for foreign sourcing prior to admitting such app onto your app store?

       a. If yes, what steps do you take to vet each app regarding foreign sourcing, including whether apps or app developers have a direct or indirect relationship with foreign governments?

       b. If no, why not?

7. Do you review each app to determine whether the app or app developer has a direct or indirect relationship with the CCP? Such relationship may include, but is not limited to, a financial stake in the company by the Chinese state, Chinese state-owned entities, or a CCP board operating within the company.

       a. If yes, what steps do you take to vet such apps?

       b. If no, why not?

8. How are apps on your app store reviewed for critical vulnerabilities?

9. Is there a review of the justifications of the level of permissions that apps seek?

If you have any questions, please contact Tim Kurth and Bijan Koohmaraie at (202) 225-3641. Thank you for your prompt attention to this request.

Sincerely,

Greg Walden
Republican Leader

Cathy McMorris Rodgers
Republican Leader
Subcommittee on Consumer Protection
  and Commerce