Congress of the United States
Washington, DC 20515

November 2, 2022

Sundar Pichai
Chief Executive Officer
Google
1600 Amphitheater Parkway
Mountain View, CA 94043

Dear Mr. Pichai:

We write to express our serious concern for consumer safety and data privacy related to Google's approval of multiple applications into its Play Store with the potential to secretly monitor users, collect sensitive personal information, and share such information with foreign entities. Google's failure to implement rigorous application scrutiny makes Americans vulnerable to foreign surveillance, particularly from adversarial actors like China.

Recent reporting revealed that several applications on the Google Play Store, including Facebook, Facebook Messenger, Instagram, and TikTok, contain code that enables these applications to closely surveil users while they are using in-app browsers.[1] The research demonstrated how TikTok's in-app browser injected code to observe all taps and keyboard inputs, which can include passwords and credit card information.[2] In June, FCC Commissioner Brendan Carr wrote to you to underscore the major data privacy and security threat posed by TikTok: "At its core, TikTok functions as a sophisticated surveillance tool that harvests extensive amounts of personal and sensitive data."[3]

TikTok is owned by Beijing-based ByteDance – an organization that is beholden to the Communist Party of China and required by Chinese law to comply with the People's Republic of China's surveillance demands. TikTok's case is particularly egregious in that it is the only major app evaluated that "doesn't even offer an option to open the link in the device's default browser, forcing you to go through its own in-app browser."[4] Turning a blind eye to an application that permits such surveillance endangers Americans, specifically the overwhelming number of teenagers that use TikTok and may be more susceptible to manipulation or negative social, emotional, and developmental impacts.[5]

Google has a responsibility to ensure that the applications on its Play Store meet minimum security criteria; however, applications with malicious features are regularly admitted into the Play Store. These failures put consumer safety and user privacy at risk. Earlier this summer,

---

[1] https://mashable.com/article/tiktok-browser-monitoring
[2] https://krausefx.com/blog/announcing-inappbrowsercom-see-what-javascript-commands-get-executed-in-an-in-app-browser
[3] https://www.reuters.com/article/tiktok-carr-fcc-idCAKBN2OA28B
[4] Ibid.
[5] https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/

security researchers discovered 36 applications with embedded malware available on the Play Store.[6] The apps were installed nearly 10 million times, and several of the apps remained available for download for days after the report was made public.[7] Another five malicious applications were discovered on the Play Store even more recently.[8] The recent revelation of security vulnerabilities related to TikTok, the most downloaded app for Android in the Google Play Store worldwide, further calls into question Google's ability to ensure marketplace safety.

Given these serious national security and public interest concerns, we request your response no later than November 30 to the following inquiries:

1. **Risks:**
    a. In Google's view, what risks do applications with in-app browsers pose to user safety and data security? Why do many applications embed this feature within their platforms? Is there another option? How is Google addressing these risks?

    b. In Google's view, what risks do applications with cross-border data transfers to U.S. adversaries including but not limited to the People's Republic of China pose to user safety and data security? How is Google thinking about these risks as a guardian of the application marketplace?

2. **Play Store Review Process:**

    a. During Google's Play Store review process, do applications with in-app browsing features get flagged by rule? If so, can you explain what this review process looks like? If not, can you explain why flagging applications with these features as a matter of course is not part of your current process and if you have plans to include this feature flag in a future iteration of your review process?

    b. During Google's Play Store review process, must applications disclose cross-border data transfers and the countries involved in such transfers, particularly to U.S. adversaries? If not, can you explain why this is not part of your current process and if you have plans to include this type of disclosure in a future iteration of your review process?

3. **Removal from Play Store:**

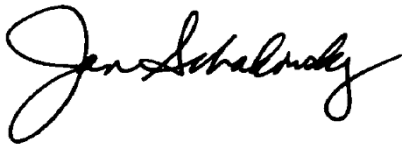
    a. Does Google plan to reevaluate or remove any applications with in-app browsers (e.g., TikTok) in light of recent reporting on user vulnerability?

    b. Does Google plan to reevaluate or remove any applications with cross-border data transfers to U.S. adversaries including but not limited to the People's Republic of China?

[6] https://www.pcmag.com/news/36-malicious-android-apps-found-on-google-play-did-you-install-them
[7] Ibid.
[8] https://www.techradar.com/news/beware-another-dangerous-android-malware-has-had-millions-of-downloads-from-the-google-play-store

Thank you for your attention to addressing deficiencies and vulnerabilities in the Play Store to better protect the digital privacy and data security of millions of individuals worldwide.

Sincerely,



Jan Schakowsky

Chair, Subcommittee on Consumer Protection and Commerce
House Committee on Energy and Commerce

Gus M. Bilirakis

Ranking Member, Subcommittee on Consumer Protection and Commerce
House Committee on Energy and Commerce