Congress of the United States
Washington, DC 20515

November 2, 2022

Tim Cook
Chief Executive Officer
Apple, Inc.
1 Infinite Loop
Cupertino, CA 95014

Dear Mr. Cook:

We write to express our serious concern for consumer safety and data privacy related to Apple's approval of multiple applications into its App Store with the potential to secretly monitor users, collect sensitive personal information, and share such information with foreign entities. Apple'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 Apple's App 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]

---

[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/

Apple has long argued that it is the only company that can offer a secure App store.[6] Last year, an Apple spokesperson stated, "We hold developers to high standards to keep the App Store a safe and trusted place for customers to download software, and we will always take action against apps that pose a harm to users."[7]

However, despite Apple's assurances to consumers, applications with concerning features, like the ones described above on TikTok, are available for download in the App Store. These failures put consumer safety and user privacy at risk. Analysis from the *Washington Post* showed that nearly two percent of the 1,000 highest-grossing apps on the App Store are scams, which have defrauded consumers to the tune of almost $50 million.[8] Earlier this summer, an independent researcher discovered seven apps of Chinese origin with embedded malware available on Apple's App Store.[9] Each of the seven apps was among the top 100 downloaded apps on the App Store, including a seemingly benign PDF reader that ranked #1 in the Education category.[10] Another 18 malicious applications were discovered on the App Store in 2019.[11] The recent revelations of security vulnerabilities related to TikTok, the most downloaded app for iPhone in the Apple App Store worldwide, further calls into question Apple's ability to ensure consumer safety.

Given Apple's stated commitment to ensure the safety of its marketplace, protect the consumers who use it, and hold developers to high standards, we request your response by November 30 to the following inquiries:

1. **Risks:**

    a. In Apple'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 Apple addressing these risks?

    b. In Apple'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 Apple thinking about these risks as a guardian of the application marketplace?

2. **App Store Review Process:**

    a. During Apple's App 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 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?

---

[6] https://www.bloomberg.com/news/articles/2022-06-23/apple-aapl-defends-app-store-security-from-new-us-antitrust-bill-critics?leadSource=uverify%20wall

[7] https://www.washingtonpost.com/technology/2021/06/06/apple-app-store-scams-fraud/

[8] https://www.washingtonpost.com/technology/2021/06/06/apple-app-store-scams-fraud/

[9] https://lifehacker.com/great-now-the-apple-app-store-has-malware-too-1849386738

[10] Ibid.

[11] https://www.wired.com/story/apple-app-store-malware-click-fraud/

b. During Apple's App 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 App Store:**

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

b. Does Apple 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?

By continuing to advocate for its exclusive control over the application marketplace on iOS devices, Apple has assumed heightened responsibility for safety of applications made available to its users. Thank you for your attention to addressing deficiencies and vulnerabilities in the App Store in order to 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