

United States Senate

July 24, 2025

Tim Cook
Chief Executive Officer
Apple Inc.
One Apple Park Way
Cupertino, CA 95014

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

Dear Messrs. Cook and Pichai:

We write to express our concern over reports that Apple and Google continue to permit free downloadable VPN applications on the App Store and Google Play Store that are owned and operated by Chinese military companies. Alarming, some of the apps are linked to a company called Qihoo 360, which was added to the Department of Commerce's Entity's List in 2020 for its ties to the People's Liberation Army (PLA).¹ Despite these glaring red flags and the publication of reports highlighting the issue more than three months ago,² Apple and Google continue to undermine national security by allowing apps that give the Chinese government access to private information of millions of Americans.³

As the United States works to respond to ongoing cyber intrusions by the PLA, including the Salt Typhoon hacks, it is unacceptable that your companies have allowed platforms with known links to the PLA to continue operating unimpeded across our cyberspace. According to a *Financial Times* article, it took outreach from their journalists for two of the five VPN apps linked to Qihoo 360, a company who is under U.S. sanctions and has been added to the Entity List, to be removed.⁴ The continued availability of these apps on your platforms for U.S. users are a trojan horse for cyberattacks and infiltration by the Chinese government, threatening the integrity of our systems and directly targeting the data of the American people.

More concerning, according to the data on the pages of the apps that are active on the platform, several apps — including those linked to Qihoo 360 — have subscriptions and in-app purchases. The fact that Apple and Google both take fees from purchases made in apps suggests your companies are also profiting from these Chinese-owned apps, including those tied to a Chinese military company that has been under U.S. Commerce sanctions for five years.⁵

¹ <https://www.federalregister.gov/documents/2020/06/05/2020-10869/addition-of-entities-to-the-entity-list-revision-of-certain-entries-on-the-entity-list>

² <https://www.techtransparencyproject.org/articles/apple-offers-apps-with-ties-to-chinese-military>
<https://www.ft.com/content/709df467-7a96-4d2a-a9f6-18242fcb0ddf>

³ <https://developer.apple.com/app-store/review/guidelines/#vpn-apps>
<https://support.google.com/googleplay/android-developer/answer/10144311?hl=en>

⁴ <https://www.ft.com/content/709df467-7a96-4d2a-a9f6-18242fcb0ddf>

⁵ <https://developer.apple.com/support/downloads/terms/schedules/Schedule-2-and-3-20240610-English.pdf>
<https://developer.apple.com/app-store/small-business-program/>

It even appears that two employees of Guangzhou Lianchuang, a subsidiary of Qihoo 360, admitted to working on foreign VPNs and confirmed their company's ties to Qihoo.⁶ Furthermore, Guangzhou Lianchuang's hiring practices reportedly include looking for the right candidate that is "well versed in American culture".⁷ This reporting is very concerning and should prompt you all to remove any VPN apps that are clearly linked to these entities.


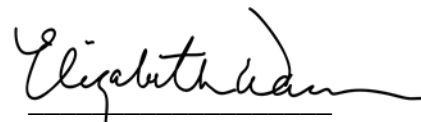
Beyond the national security implications, the continued presence of these apps raises serious questions about Apple and Google's carefully cultivated reputations for protecting users' privacy. Your company has repeatedly claimed it maintains strict control over its app store, to protect user's privacy and security.⁸ Yet lapses like the ones identified in this letter demonstrate that your company is failing users and the broader public. We are also aware that Apple has previously removed apps to censor the App Store at the behest of the Chinese government.⁹

We want to understand why your companies continue to offer VPN apps that pose a threat to U.S. national security. To that effect, we request written responses to the following:

- The rationale for maintaining these VPN apps on your platforms;
- The number of American-based downloads for these apps from your platforms;
- Your verification processes for these entities distributing VPN service;
- The revenue your companies have earned from in-app purchases linked to these Chinese companies, including Qihoo 360; and
- Whether your teams have notified any relevant federal government entities or law enforcement agencies about these platforms.

We trust you will agree that leaving our country vulnerable to cyber infiltration is not in our collective interest. The People's Republic of China continues to undermine U.S. cybersecurity by supporting entities that have, or are actively attempting to, damage the integrity of our critical infrastructure. Attempts to access the personal data of Americans—especially minors—are particularly troubling. We hope to work together to root out this growing threat.

Sincerely,


Eric Schmitt
United States Senator
Elizabeth Warren
United States Senator

<https://support.google.com/googleplay/android-developer/answer/112622?hl=en>

⁶ <https://www.techtransparencyproject.org/articles/apple-offers-apps-with-ties-to-chinese-military>

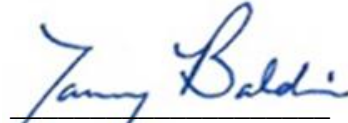
⁷ [Ibid.](#)

⁸ <https://arstechnica.com/gaming/2021/05/epic-vs-apple-trial-starts-today-heres-what-to-expect/>

⁹ <https://www.techtransparencyproject.org/articles/apple-censoring-its-app-store-china>




Marsha Blackburn
United States Senator



Tammy Baldwin
United States Senator



Pete Ricketts
United States Senator



Mark Kelly
United States Senator



Joni Ernst
United States Senator