CAROLYN B. MALONEY
CHAIRWOMAN

ONE HUNDRED SIXTEENTH CONGRESS

JIM JORDAN, OHIO
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
http://oversight.house.gov

July 14, 2020

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

Dear Mr. Cook,

Thank you for Apple's letter dated January 10, 2020, responding to the Subcommittee's questions about the potential national security risks of foreign owned and operated smartphone applications. In the response, Apple indicated that consumers using the AppStore are ultimately responsible for the information they choose to share with third-party applications on their smartphone devices. The response also stated that Apple "does not require information on where user data (if any such data is collected by the developer's app) will be housed."[1]

While the Subcommittee appreciates the safeguards Apple has put in place to protect user privacy, we remain concerned that mobile applications owned or operated by foreign developers, or that store the user data of U.S. citizens overseas, could enable our adversaries to access significant quantities of potentially sensitive information on American citizens without their knowledge to the detriment of U.S. national security.

In February 2020, the Subcommittee wrote to Acting Director of National Intelligence Richard Grenell and Federal Bureau of Investigation (FBI) Director Christopher Wray seeking their agencies' views about the potential national security risks of foreign owned and operated smartphone applications.[2]

On July 7, 2020, the Office of the Director of National Intelligence (ODNI) reinforced the Subcommittee's concerns, stating:

---

[1] Letter from Timothy Powderly, Director of Federal Affairs, Apple, to Chairman Stephen F. Lynch, Subcommittee on National Security, Committee on Oversight and Reform (Jan. 10, 2020).

[2] Letter from Chairman Stephen F. Lynch, Subcommittee on National Security, to Director Christopher Wray, Federal Bureau of Investigation, and Acting Director Richard Grenell, Director of National Intelligence, (Feb. 26, 2020) (online at https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2020-02-26%20SFL%20to%20ODNI%20FBI%20re%20Apps.pdf).

> Mobile applications developed, operated or owned by foreign entities present a potential national security risk because developers can deliberately code *kill switches*, *backdoors* or vulnerable data streams into mobile applications that allow access to the application's software, application-generated data, or even—in some cases—the device itself, and because application owners/operators can filter, censor, corrupt, intercept, and illegitimately divert or share data generated by applications.[3]

ODNI reported that "Generally, the key risk factors from foreign-developed applications are":

- Clear foreign government intent to harm U.S. interests;
- Technical skills and capabilities that would enable them to conduct supply chain operations;
- The nature of the information produced, collected, or stored by an application. For example, an application that stores and/or accesses users' sensitive communications or personal information may incur higher risks than an application that stores only the user's progress in a game;
- A legal/governance regime that would enable the foreign country to easily utilize commercial application developers for their foreign intelligence operations.[4]

In its own July 10, 2020, response, the FBI told the Subcommittee:

> [I]f users voluntarily provide information to a mobile application that is based in a foreign country or that stores information in a foreign country, the information is subject to the respective foreign country's laws, which may allow its acquisition by that country's government.[5]

To address these potential threats, some countries have passed legislation to require internet companies to store data collected about their citizens on local servers, while others have sought to ban foreign smartphone applications altogether.[6] Yet these policies also come with significant costs by inhibiting innovation, enabling censorship, and restricting the movement of ideas across a free and open internet.

---

[3] Letter from Office of Director of National Intelligence to Chairman Stephen F. Lynch, Subcommittee on National Security, Committee on Oversight and Reform (July 7, 2020) (online at https://oversight.house.gov/sites/democrats.oversight.house.gov/files/Unclassified%20NCSC%20Info%20for%20Rep%20Lynch_0.pdf).

[4] *Id.*

[5] Letter from Assistant Director Jill C. Tyson, Federal Bureau of Investigation (July 10, 2020) (online at https://oversight.house.gov/sites/democrats.oversight.house.gov/files/20200710_FBI_Response_to_Chairman_Lynch_incoming_20200226.pdf).

[6] See *Russia to Block LinkedIn Over Data-Privacy Dispute*, Wall Street Journal (Nov. 10, 2016) (online at www.wsj.com/articles/russia-may-block-linkedin-if-company-loses-court-case-on-personal-data-law-1478775414); *India Bans 59 Mostly Chinese Apps Amid Border Crisis*, Reuters (June 29, 2020) (online at www.reuters.com/article/us-india-china-apps/india-bans-59-mostly-chinese-apps-amid-border-crisis-idUSKBN24025V).

As an industry leader, Apple can and must do more to ensure that smartphone applications made available to U.S. citizens on the AppStore protect stored data from unlawful foreign exploitation, and do not compromise U.S. national security. At a minimum, Apple should take steps to ensure that users are aware of the potential privacy and national security risks of sharing sensitive information with applications that store data in countries adversarial to the United States, or whose developers are subsidiaries of overseas companies.

For these reasons, please provide answers to the following questions by July 31, 2020:

1. In its January 10, 2020, letter, Apple advised that it is not aware of any statutory or regulatory limitations that would prohibit it from requiring application developers to provide the locations where user data will be stored.

    a. Will Apple commit to requiring developers to disclose the countries in which they store user data collected by their applications?

    b. Will Apple commit to making this information available to consumers in its application listings on the AppStore?

2. Will Apple commit to requiring developers to disclose whether they are a corporate subsidiary of a foreign entity? Will Apple commit to making this information available to consumers in its application listings on the AppStore?

3. Has Apple previously removed a third-party application from the AppStore due to suspicious or nefarious exploitation of user data by foreign governments? Please describe the circumstances; and

4. Does Apple have additional recommendations that would better protect user data stored on third-party applications from foreign collection and exploitation? For example, would Apple consider notifying users in the AppStore if certain applications collect especially personal or sensitive information?

The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051.

Sincerely,

Stephen F. Lynch
Chairman
Subcommittee on National Security

cc: The Honorable Glenn Grothman, Ranking Member
Subcommittee on National Security