

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>

December 13, 2019

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

Dear Mr. Cook,

Recent press reports have shed light on allegations that certain foreign companies and developers may be providing sensitive data on U.S. citizens via their mobile applications to their host governments, thereby creating significant national security risks.¹ Given these concerns, the Subcommittee seeks information relating to whether Apple requires mobile application developers to disclose their potential overseas affiliations prior to making their products available on the Application Store.

U.S. laws permit mobile applications to collect massive amounts of personal information about their users as long as the users consent to the collection of that information as a condition of service. However, many smartphone owners are not aware that by consenting to an application's service agreement, they are authorizing the application to access significant quantities of personal, and oftentimes sensitive, information. The extent to which this information is secured, either through encryption or alternative mechanisms, as well as the degree to which user data is shared, varies across applications.

When using mobile devices in the United States, users may assume that the Fourth Amendment, which prohibits unreasonable government searches and seizures, protects the data that they share voluntarily with the mobile applications on their smartphones. However, when a mobile application is owned, operated, or developed by a foreign entity—irrespective of whether that data is stored on servers in the United States or abroad—there is a greater risk that foreign governments might be able to access that information. This could happen if the foreign

¹ See *Exclusive: U.S. Opens National Security Investigation into TikTok—Sources*, Reuters (Nov. 1, 2019) (online at www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-u-s-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL); *Why is the U.S. Forcing a Chinese Company to Sell the Gay Dating App Grindr?*, Washington Post (Apr. 3, 2019) (online at www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr/); *The FBI Investigated FaceApp. Here's What It Found*, Forbes (Dec. 3, 2019) (online at www.forbes.com/sites/kateoflahertyuk/2019/12/03/fbi-faceapp-investigation-confirms-threat-from-apps-developed-in-russia/#55f216ba45bc).

government gains unauthorized access to a mobile application's information technology systems or if the government compels or incentivizes developers to share their user data.

For example, according to American University Law Professor Jennifer Daskal and New America Fellow Samm Sacks, while China does not have automatic access to data stored by Chinese-owned companies, "the reality is that if and when Beijing makes a demand, it is hard for Chinese-based companies to say no."²

Similarly, in a November 2019 letter to Senate Minority Leader Charles Schumer, Jill C. Tyson, Assistant Director of the Federal Bureau of Investigation (FBI) Office of Congressional Affairs, stated:

The FBI considers any mobile application or similar product developed in Russia ... to be a potential counterintelligence threat, based on the data the product collects, its privacy and terms of use policies, and the legal mechanisms available to the Government of Russia that permit access to data within Russia's borders.³

Given the pervasiveness of smartphone technology in the United States, as well as the vast amounts of information stored on those devices, foreign adversaries may be able to collect sensitive information about U.S. citizens, which presents serious and immediate risks for U.S. national security.

For example, by collecting personal information on U.S. government personnel who have access to classified information, foreign adversaries may attempt to expose them to blackmail, tailor intelligence spotting or recruitment activities to specific targets, or exert undue foreign influence in U.S. policymaking. In addition, artificial intelligence could enable foreign adversaries to manipulate user-provided data to create profiles on average U.S. citizens that could be leveraged in future military conflicts or diplomatic disputes.⁴

Congress has a responsibility to protect the privacy of American citizens and the national security of the United States while foreign entities and governments invest in economic and technological advancement. Deliberate, thorough, and transparent oversight of foreign operated mobile applications promotes these goals. The Committee on Foreign Investment in the United States' ongoing investigation into TikTok and their previous determination that Chinese-owned Kunlun must divest ownership in the popular LGBTQ dating application, Grindr, are important

² *The Furor Over TikTok is About Something Much Bigger*, Slate (Nov. 8, 2019) (online at <https://slate.com/technology/2019/11/tiktok-bytedance-china-geopolitical-threat.html>).

³ Letter from Jill C. Tyson, Assistant Director, Federal Bureau of Investigation Office of Congressional Affairs, to Senator Charles E. Schumer, Senate Minority Leader (Nov. 25, 2019) (online at www.democrats.senate.gov/imo/media/doc/FBI%20Letter%20to%20Schumer%20re%20FaceApp11.pdf).

⁴ Following the breach of Office of Personnel Management computer systems in December 2014, the Washington Post reported in June 2015 reported that China is building "massive databases of Americans' personal information." See *With a Series of Major Hacks, China Builds a Database on Americans*, Washington Post (Jun. 5, 2019) (online at www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html).

examples of such oversight. However, this may be only a small example of how foreign adversaries might seek to exploit consumer mobile application data to gain leverage over the United States and its citizens.

For these reasons, please provide answers to the following questions by January 10, 2020:

1. How does Apple determine whether an application should be made available to the public on the App Store?
2. What information does Apple require application developers to submit with their proposals?
3. Does Apple require developers to disclose the country (or countries) in which their mobile applications will house user data?
 - a. If so, does Apple determine whether to list certain applications on the App Store based on where user data will be housed?
 - b. If not, are there any statutory or regulatory limitations that prohibit Apple from requesting this information?
4. Does Apple require developers to disclose when a non-U.S. corporation or entity owns a greater than 50 percent equity stake in an application?
 - a. If so, does Apple determine whether to list certain applications on the App Store based on foreign corporate ownership?
 - b. If not, are there any statutory limitations that prohibit Apple from requesting this information?
5. Has Apple established baseline data protection standards that mobile application proposals must comply with?
6. According to Apple's App Store Review Guidelines, "Apps that share user data without user consent or otherwise complying with data privacy laws may be removed from sale and may result in ... removal from the Apple Developer Program."⁵ How does Apple determine whether mobile applications pending approval operate in accordance with their user consent agreements or privacy policies? Does Apple have a mechanism for periodically reviewing and enforcing these agreements and policies?
7. Does Apple track an application's total number of downloads in the United States?

⁵ Apple, *App Store Review Guidelines* (online at <https://developer.apple.com/app-store/review/guidelines/>).

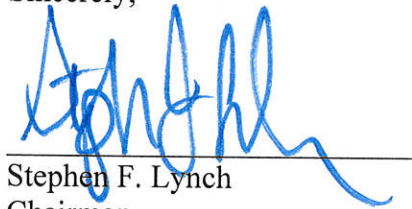
Mr. Timothy Cook
Page 4

8. Does Apple track an application's potential number of users in the United States?

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

Enclosure

cc: The Honorable Jody B. Hice, Ranking Member
Subcommittee on National Security

Responding to Committee Document Requests

1. In complying with this request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. Produce all documents that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party.
2. Requested documents, and all documents reasonably related to the requested documents, should not be destroyed, altered, removed, transferred, or otherwise made inaccessible to the Committees.
3. In the event that any entity, organization, or individual denoted in this request is or has been known by any name other than that herein denoted, the request shall be read also to include that alternative identification.
4. The Committees' preference is to receive documents in electronic form (i.e., CD, memory stick, thumb drive, or secure file transfer) in lieu of paper productions.
5. Documents produced in electronic format should be organized, identified, and indexed electronically.
6. Electronic document productions should be prepared according to the following standards:
 - a. The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - b. Document numbers in the load file should match document Bates numbers and TIF file names.
 - c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - d. All electronic documents produced to the Committees should include the following fields of metadata specific to each document, and no modifications should be made to the original metadata:

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,

INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,
BEGATTACH.

7. Documents produced to the Committees should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, zip file, box, or folder is produced, each should contain an index describing its contents.
8. Documents produced in response to this request shall be produced together with copies of file labels, dividers, or identifying markers with which they were associated when the request was served.
9. When you produce documents, you should identify the paragraph(s) or request(s) in the Committees' letter to which the documents respond.
10. The fact that any other person or entity also possesses non-identical or identical copies of the same documents shall not be a basis to withhold any information.
11. The pendency of or potential for litigation shall not be a basis to withhold any information.
12. In accordance with 5 U.S.C. § 552(d), the Freedom of Information Act (FOIA) and any statutory exemptions to FOIA shall not be a basis for withholding any information.
13. Pursuant to 5 U.S.C. § 552a(b)(9), the Privacy Act shall not be a basis for withholding information.
14. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
15. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) every privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, addressee, and any other recipient(s); (e) the relationship of the author and addressee to each other; and (f) the basis for the privilege(s) asserted.
16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (by date, author, subject, and recipients), and explain the circumstances under which the document ceased to be in your possession, custody, or control.
17. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents that would be responsive as if the date or other descriptive detail were correct.

18. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data, or information not produced because it has not been located or discovered by the return date shall be produced immediately upon subsequent location or discovery.
19. All documents shall be Bates-stamped sequentially and produced sequentially.
20. Two sets of each production shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee on Oversight and Reform, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2105 of the Rayburn House Office Building. When documents are produced to the Committee on Financial Services, production sets shall be delivered to the Majority Staff in Room 2129 of the Rayburn House Office Building and the Minority Staff in Room 4340 of the O'Neill House Office Building. When documents are produced to the Permanent Select Committee on Intelligence, production sets shall be delivered to Majority and Minority Staff in Room HVC-304 of the Capital Visitor Center.
21. Upon completion of the production, submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control that reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, data, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, communications, electronic mail (email), contracts, cables, notations of any type of conversation, telephone call, meeting or other inter-office or intra-office communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a

part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, mail, releases, electronic message including email (desktop or mobile device), text message, instant message, MMS or SMS message, message application, or otherwise.
3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information that might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neutral genders.
4. The term “including” shall be construed broadly to mean “including, but not limited to.”
5. The term “Company” means the named legal entity as well as any units, firms, partnerships, associations, corporations, limited liability companies, trusts, subsidiaries, affiliates, divisions, departments, branches, joint ventures, proprietorships, syndicates, or other legal, business or government entities over which the named legal entity exercises control or in which the named entity has any ownership whatsoever.
6. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual’s complete name and title; (b) the individual’s business or personal address and phone number; and (c) any and all known aliases.
7. The term “related to” or “referring or relating to,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with, or is pertinent to that subject in any manner whatsoever.
8. The term “employee” means any past or present agent, borrowed employee, casual employee, consultant, contractor, de facto employee, detailee, fellow, independent contractor, intern, joint adventurer, loaned employee, officer, part-time employee, permanent employee, provisional employee, special government employee, subcontractor, or any other type of service provider.
9. The term “individual” means all natural persons and all persons or entities acting on their behalf.