

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>

February 26, 2020

The Honorable Christopher A. Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535-0001

The Honorable Richard A. Grenell
Acting Director of National Intelligence
Office of the Director of National Intelligence
1500 Tysons McLean Drive
McLean, V.A. 22102

Dear Director Wray and Acting Director Grenell:

The Subcommittee on National Security is seeking information related to whether and how certain foreign mobile application companies and developers might be providing sensitive data on U.S. citizens to their host governments. Given the pervasiveness of smartphone technology in the United States, as well as the vast amounts of information stored on those devices, the Subcommittee is concerned that foreign adversaries may be collecting sensitive information about U.S. citizens, which presents serious and immediate risks for U.S. national security.

On December 13, 2019, the Subcommittee wrote to Apple and Google requesting information related to whether they require mobile application developers to disclose their potential overseas affiliations prior to making their products available on their respective digital marketplaces.¹

In its January 10, 2020, response, Apple confirmed that although the company “requires developers to submit the country that their legal entity is located in,” it does not require “information on where user data (if any such data is collected by the developer’s app) will be

¹ Letter from Chairman Stephen F. Lynch, Subcommittee on National Security, Committee on Oversight and Reform, to Timothy Cook, Chief Executive Officer, Apple (Dec. 13, 2019) (online at <https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2019-12-13.SFL%20to%20Cook-Apple%20re%20Mobile%20Apps.pdf>); Letter from Chairman Stephen F. Lynch, Subcommittee on National Security, Committee on Oversight and Reform, to Sundar Pichai, Chief Executive Officer, Google (Dec. 13, 2019) (online at <https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2019-12-13.SFL%20to%20Pichai-Google%20re%20Mobile%20Apps.pdf>).

housed.” Apple confirmed that it “does not decide what user data a third-party app can access, the user does.”²

Similarly, in its January 17, 2020, response, Google stated that it does “not require developers to provide the countries in which their mobile applications will house user data” and acknowledged that “some developers, especially those with a global user base, may store data in multiple countries.”³

U.S. laws permit mobile applications to collect massive amounts of personal information if their 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 may be authorizing the application to access significant quantities of personal, and often sensitive, information. In other words, by consenting to a mobile application’s privacy policy, U.S. citizens may be surrendering virtually limitless quantities of information.

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 they share voluntarily with the mobile applications on their smartphones. However, when a mobile application is owned, operated, or developed by a foreign entity, or when the data it collects is stored on servers outside the United States, there is a greater risk that foreign governments might be able to access that information for nefarious purposes. This could happen if the foreign government gains unauthorized access to a mobile application’s information technology systems or if the government compels or incentivizes developers to share user data.

The Federal Bureau of Investigation (FBI) has previously confirmed that mobile applications developed in Russia could present a counterintelligence threat. In a November 2019 letter to Senate Minority Leader Charles Schumer, the FBI wrote:

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.⁴

The Subcommittee is deeply concerned that foreign governments, particularly U.S. adversaries, might be exploiting our relatively lenient domestic privacy laws to gain a national

² 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).

³ Letter from Mark Isakowitz, Vice President of Government Affairs and Public Policy, Google, to Chairman Stephen F. Lynch, Subcommittee on National Security, Committee on Oversight and Reform (Jan. 17, 2020).

⁴ 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).

security or counterintelligence advantage. For all these reasons, I respectfully request that you provide responses to the following questions by March 13, 2020:

1. Does the U.S. Intelligence Community (IC) assess that mobile applications developed, operated, or owned by foreign entities are a potential national security risk?
2. Does the IC assess that mobile applications that store or house information about U.S. citizens overseas are a potential national security risk?
3. Are there particular countries that the IC and the FBI assess to be exploiting or leveraging mobile applications to collect information on U.S. citizens?
4. Are there particular mobile applications, developers, or companies that the IC and the FBI assess to be willfully sharing information on U.S. citizens with foreign governments?
5. Are there particular mobile applications, developers, or companies that the IC and the FBI assess to be especially vulnerable to undue foreign government influence?
6. Does the FBI have a mechanism for notifying mobile application owners, developers, and operators that their products have been compromised by a foreign government?
7. Does the FBI have a mechanism for notifying digital marketplace administrators, including but not limited to Apple and Google, that particular mobile applications on their platforms have been compromised by a foreign government?
8. Does the FBI have a mechanism for notifying consumers and users of mobile applications that particular applications have been compromised by a foreign government?

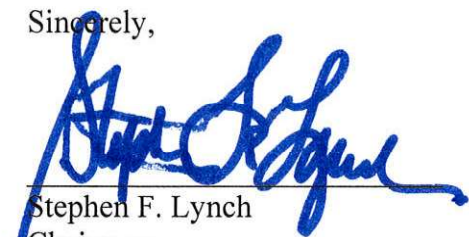
To the extent possible, please provide your answers in an unclassified format, as the American people have the right to know how our adversaries might be collecting the personal data they share on their mobile devices.

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 additional information related to the subject matter of this letter, or questions regarding this request, please contact Subcommittee staff at (202) 225-5051.

The Honorable Christopher A. Wray
The Honorable Richard A. Grenell
Page 4

Sincerely,

A handwritten signature in blue ink, appearing to read "Stephen F. Lynch", is written over a horizontal line.

Stephen F. Lynch
Chairman
Subcommittee on National Security

Enclosure

cc: The Honorable Jody B. Hice, Ranking Member

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.