

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

July 9, 2018

Larry Page
Chief Executive Officer
Alphabet, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043-13514

Dear Mr. Page:

The Energy and Commerce Committee is reviewing business practices that may impact the privacy expectations of Americans. We write today to learn more about the capabilities of Google's Android devices, in particular the collection and use of consumer data and microphone functionality of Android phones. Recent reports have indicated that consumer data, including location information, recordings of users, and email contents, may be used in ways that consumers do not expect. We seek Google's assistance in understanding the accuracy of these reports.

According to media reports published in November 2017, Android phones collect information on nearby cellular towers even if location services, WiFi, and Bluetooth capabilities are disabled, no third-party apps are installed or running, and the phones lack subscriber identification module (SIM) cards.¹ The report explained that this information is held locally on the phone until network capabilities are reestablished, at which point the data is sent to Google.² Additional information provided to the Committee suggests that this behavior is not limited to cellular tower data but is also gathered for nearby WiFi hotspots and Bluetooth beacons. Other behaviors that could have an impact on consumer protection issues were also raised, such as the fact that reenabling location services for one app on an Android phone reenables location services for all apps on that phone.

¹ Keith Collins, *Google collects Android users' locations even when location services are disabled*, QUARTZ (Nov. 21, 2017), <https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/>.

² *Id.*

Android users have a reasonable expectation of privacy when taking active steps to prevent being tracked by their device. Considering that many consumers likely believe that a phone that lacks a SIM card, or one for which they have affirmatively disabled location services, WiFi, or Bluetooth – such as through turning on “Airplane Mode” – is not actively tracking them, this alleged behavior is troubling.

Recent reports have also suggested that smartphone devices can, and in some instances, do, collect “non-triggered” audio data from users’ conversations near a smartphone in order to hear a “trigger” phrase,³ such as “okay Google”⁴ or “hey Siri.”⁵ It has also been suggested that third party applications have access to and use this “non-triggered” data without disclosure to users.

Changes to the Google Play Store terms, including the Safe Browsing changes,⁶ announced in December 2017, significantly increased required disclosures to users by third-party apps about data collection and use practices.⁷ Improving disclosures for users should remain a goal for the entire ecosystem, but it is of particular note when one of the two major app platforms updates requirements for third-party app developers confirming the control that can be exercised over which apps are available to users and their functionality.

In a similar circumstance, in June 2017, Google announced changes to Gmail that would halt scanning the contents of a user’s email to personalize advertisements to “keep privacy and security paramount.”⁸ Last week, reports surfaced that in spite of this policy change, Google still permitted third parties to access the contents of users’ emails, including message text, email signatures, and receipt data, to personalize content.⁹ In the context of free services offered by third parties, these practices raise questions about how representations made by a platform are carried out in practice.

Therefore, pursuant to Rules X and XI of the United States House of Representatives, we ask that you respond to the following questions by no later than July 23, 2018:

³ See Sam Nichols, *Your Phone Is Listening and it's Not Paranoia*, VICE NEWS, June 4, 2018, available at https://www.vice.com/en_au/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia.

⁴ Google Search Help, *Use “Ok Google” on Android*, <https://support.google.com/websearch/answer/6031948?hl=en&co=GENIE.Platform%3DAndroid> (last accessed June 22, 2018).

⁵ Apple, *The Basics*, <https://www.apple.com/ios/siri/> (last accessed June 22, 2018).

⁶ Google, *Safe Browsing*, <https://safebrowsing.google.com/> (last accessed June 22, 2018).

⁷ Brandon Vigliarolo, *Google’s new app privacy standards mean big changes for developers*, TECHREPUBLIC, December 4, 2017, available at <https://www.techrepublic.com/article/googles-new-app-privacy-standards-mean-big-changes-for-developers/>.

⁸ Jack Nicas, *Google to Stop Reading Users’ Emails to Target Ads*, THE WALL STREET JOURNAL, June 23, 2017, available at https://www.wsj.com/articles/google-to-stop-reading-users-emails-to-target-ads-1498247136?mod=article_inline.

⁹ Douglas MacMillan, *Tech’s ‘Dirty Secret’: The App Developers Sifting Through Your Gmail*, THE WALL STREET JOURNAL, July 2, 2018, available at https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442?shareToken=st16ef993b912947ec866f77f24e4417c9&ref=article_email_share.

1. When an Android phone lacks a SIM card, is that phone programmed to collect and locally store information through a different data-collection capability, if available, regarding:
 - a. Nearby cellular towers;
 - b. Nearby WiFi hotspots; or,
 - c. Nearby Bluetooth beacons?
2. If the answers to any of the preceding questions are “yes,” are Android phones lacking SIM cards programmed to send this locally-stored information to Google when one or more networking capabilities are established?
3. When the WiFi capabilities on an Android phone are disabled, is that phone programmed to collect and locally store information through a different data-collection capability, if available, regarding:
 - a. Nearby cellular towers;
 - b. Nearby WiFi hotspots; or,
 - c. Nearby Bluetooth beacons?
4. If the answers to any of the preceding questions are “yes,” are Android phones with disabled WiFi programmed to send this locally-stored information to Google when one or more networking capabilities are established?
5. When the Bluetooth capabilities on an Android phone are disabled, is that phone programmed to collect and locally store information through a different data-collection capability, if available, regarding:
 - a. Nearby cellular towers;
 - b. Nearby WiFi hotspots; or,
 - c. Nearby Bluetooth beacons?
6. If the answers to any of the preceding questions are “yes,” are Android phones with disabled Bluetooth programmed to send this locally-stored information to Google when one or more networking capabilities are established?
7. When the location services capabilities on an Android phone are disabled, is that phone programmed to collect and locally store information through a different data-collection capability, if available, regarding:
 - a. Nearby cellular towers;
 - b. Nearby WiFi hotspots; or,
 - c. Nearby Bluetooth beacons?

8. If a consumer using an Android phone has disabled location services for multiple apps, but then reenables location services for one app, are Android phones programmed to reenable location services for all apps on that phone?
 - a. If yes, how is this reenabling of locations services for all apps disclosed to a user?
 - b. Why has Google chosen not to allow location services to be turned on individually for specific apps and not others – an all or nothing approach?
9. Do Google's Android devices have the capability to listen to consumers without a clear, unambiguous audio trigger?
 - a. If yes, how is this data used by Google or other Alphabet companies? Please describe any use or storage of these data.
 - b. If yes, what access to this data does Google give to third parties, including app developers? Please describe and include screen shots of disclosures as appropriate.
 - c. If yes, has Google considered using a visual, or other alert, to let consumers know when a devices' microphone is recording? Please describe why, or why not, such an alert is, or is not, provided on Android smartphones or other smart devices running on an Android operating system.
10. Do Google's Android devices collect audio recordings of users without consent?
 - a. If no, please include screen shots and links to public disclosures made to users about this collection.
11. Please provide copies of all of Google's policies for data collection via the microphone, or via the WiFi, Bluetooth, or cellular network capabilities on Google's Android devices.
12. Please provide Google's policies as they pertain to third party access and use, including but not limited to app developers and developer guidelines, of any data collected via the microphone, particularly data not accompanied by the "trigger" phrase "okay Google," or via the WiFi, Bluetooth, or cellular network capabilities on Google's Android devices.
13. Could Google control or limit the data collected by third-party apps available on the Google Play Store?
 - a. Please provide a list of all data elements that can be collected by a third-party app downloaded on an Android device about a user, including but not limited to contact lists stored on the Android device and location information generated by the Android device.

14. What limits does Google place on third-party app developers' ability to collect information about users' or from users' devices? Please describe in detail changes made in June 2017 from prior policies.
15. How does Google monitor and evaluate whether third-party apps are following the Google Play rules?
 - a. Have any companies ever been suspended or banned from Google Play for violating the Google Play rules?
 - b. In those cases, if any exist, were users notified that their data was misused in violation of the Google Play rules?
 - c. If yes, please provide any screen shots of such notification and a description of the conditions under which such a notification would be sent by Google.
 - d. What recourse does Google provide for users' when their data is misused in such a case?
16. What data and information does Google provide to outside software developers, or allow outside software developers to access, regarding or relating to Gmail users?
17. How many outside software developers, or third parties, are permitted to access a user's email contents with or without consent on Gmail?
 - a. Please provide a comprehensive list of the companies with access to a user's email contents on Gmail. Please specify which companies obtain consent through their terms of service and those, if any, that do not obtain consent.
 - b. Please describe the process for reviewing and approving third party access to user's email contents on Gmail?
 - c. What restrictions, if any, does Google place on how data from Gmail users may be used?
 - d. What additional steps, if any, are taken by Google to verify that the activity of companies granted access to user's email contents meets Google's terms of service?
18. Please provide Google's policies as they pertain to third party access and use, including but not limited to app developers and developer guidelines, of any data or information collected from a user's email contents on Gmail.

Please also make arrangements to provide Committee staff with a briefing on these topics. An attachment to this letter provides additional information about responding to the Committee's request. If you have any questions, please contact Melissa Froelich, Robin Colwell, or Jen Barblan of the Committee staff at (202) 225-2927. Thank you for your prompt attention to this request.


Sincerely,



Greg Walden
Chairman



Gregg Harper
Chairman
Subcommittee on Oversight
and Investigations



Marsha Blackburn
Chairman
Subcommittee on Communications
and Technology



Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

Attachment