

United States Senate

WASHINGTON, DC 20510

May 11, 2018

The Honorable Joseph Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairman Simons:

We write to bring to your attention our concerns regarding Google's collection of sensitive location data within its "Location History" service, and to urge you to investigate any deceptive acts and practices associated with the product. As recent events have demonstrated, the American public is increasingly concerned about the stockpiling of intimate data on their personal lives unknowingly collected from their online accounts and devices. Based on our investigation and public reports on Location History, we have significant reservations about Google's failure to clearly account for how that location data is collected and used by the company.

Since 2009, Google has promoted continuous tracking of user location within several of its products through a service now called Location History. When a user enables Location History, they not only provide Google with periodic data from one device, they deepen the volume and invasiveness of collection across devices and on a continuous basis. While Google describes the tracking as an opt-in feature, our own investigation found that the consent process frequently mischaracterizes the service and degrades the functionality of products in order to push users into providing permission. This conflicts with recent industry-wide changes to improve privacy on smartphones, particularly where Google forces users on Apple devices to enable more permissive settings. Moreover, Google does not offer full and accessible information to consumers on the use of their data, including in advertising and commercial analytics services. These factors raise serious questions about whether users are able to provide informed consent.

Based on our longstanding concerns regarding digital tracking, we wrote to Google demanding a full explanation of their collection of location data on December 1, 2017 (Attachment 1). Google replied in a letter dated January 12, 2018 (Attachment 2).

There has been a long established, bipartisan recognition that precise geolocation data is sensitive—raising expectations of user consent and notification. This means there should be clear opt-in consent to collect this information. Yet, Google's policies, documentation, and response

letter raise questions about their characterization of basic consumer protection terms such as “opt-in”, “opt-out”, “notice”, “consent”, and “anonymization.” Google claims Google Location History is opt-in, but both the device and application settings on Android phones frequently pushes users into providing “consent.” Often the actual user choice is a screen that provides two choices, neither of which is a clear “No” (see Attachment 3). This set of options is inadequate and the confusing consent process is replicated throughout Android’s various settings, where location privacy is often mischaracterized or subdivided so few users could effectuate their choice to opt-out of Google’s location data gathering (see Attachment 4).

In January, *Quartz* published a detailed article on the service and Google’s failure to provide an effective opt out of collection.¹ *Quartz*’s technical investigation found that when Location History is enabled, Google reported back even more device sensor information than usual, including barometric pressure, wireless signal information, battery status, and a determination about how the user is moving (such as whether they are on a bicycle). In its response letter, Google acknowledged that when Location History is on, it stores additional information from publicly-available Bluetooth “beacons,” low-power devices intended to provide proximity experiences to businesses.² These sensors provide Google with not simply an understanding of what city a user is currently in, but the exact floor and movements within a building.

Once a user allows Location History in one application, they enter into the expansive and continuous collection of location data that is not adequately communicated to users. Google describes Location History as an ‘account-level setting,’ which means that Google defaults to collection across all devices that a user is logged into. This data is collected from users even when an individual is not actively using a Google application.³ On Apple’s iOS devices, Google forces users to downgrade privacy settings that would otherwise only allow tracking when an app is open in order to use features that require Location History – effectively, users have to allow Google to always track them or not use the features at all. Since Google does not provide periodic reminders or clear indication that Location History is on, users can easily enable the service and have their location monitored well beyond their intended use of the application.

Our concerns regarding Google’s push for location tracking are exacerbated by the company’s opacity regarding the use of this data. Consumers have a right to know how their sensitive information is used, particularly when it comes to commercial purposes. Google typically describes Location History as a service to provide “better results and recommendations

¹ Yanofsky, David. “If You’re Using an Android Phone, Google May Be Tracking Every Move You Make.” *Quartz*. January 24, 2018. <https://qz.com/1183559/if-youre-using-an-android-phone-google-may-be-tracking-every-move-you-make/>.

² Letter from Molinari, Susan (Google). Received by Senators Blumenthal and Markey, 12 Jan. 2018: “There are other Google products that may scan and collect certain information from Bluetooth beacons near the device. This includes information that any Bluetooth beacon may be publicly broadcasting for use, such as beacon type, beacon identifier, signal strength, and broadcast power. For example, if a user has turned on the opt-in Location History feature for their Google account, Google will use publicly available beacon information as one signal to help determine location.”

³ “When you turn on Location History, Google remembers your location on all devices where you’re signed in, even when you’re not using the app.” from “View or Edit Your Timeline.” Google Maps Help. <https://support.google.com/maps/answer/6258979?co=GENIE.Platform%3DAndroid&hl=en>.

on Google products,” offering an example of recommending new places or giving traffic predictions. Google does not provide a full and explicit account of its use of the Location History in products and services, only including mentions of improving “location accuracy” and “battery life.”⁴ Further information is often only found in passing reference across disparate and unrelated product information pages intended for different audiences.

For example, in its “Business Help” page, Google states that Location History is used to provide information for businesses on Maps and Search related to popular times, wait times, and visit duration.⁵ This disclosure is not offered to consumers. Google makes no mention of the use of Location History for advertising purposes in its consent mechanisms, despite the fact that it clearly uses this data for ad targeting and analytics. A general purpose “Why you may see particular ads” page states that Google uses location information in ad products to infer demographic information. While that page does not disclose how it infers location, another help page includes an example scenario that indicates Location History data is used in targeting of advertisements:⁶

Dorothy gives her mailing address to an online athletics store when she buys a pair of sneakers. This athletics store puts Dorothy's mailing address in its customer database, then shares its list of mailing addresses with Google. Google matches this list with addresses associated with Google accounts (ex: addresses saved in Google Maps, or addresses from location history [emphasis added]). Later, when Dorothy is signed in to Google and is browsing online, she may see an ad from the athletics store.

This example describes the AdWords Customer Match service that allows advertisers to upload their list of customers to continue to target them as they browse the Internet.⁷

While many of the practices described implicates further consumer protection and privacy concerns, the troubling potential of this tracking is exemplified within the description of Google’s “store visits” advertisement service:⁸

Store visits are measured exclusively using data from Google users who have activated Location History, which provides a location timeline, stored against the user's Google Account. Google correlates the observed store visits from those users who have activated Location History with those users' ad clicks and then uses that data to estimate the aggregate number of store visits for all users who clicked on the advertiser's ads.

In December 2014, Google announced Store Visits analytics to provide aggregated reports of visits to retail locations by Google users who had clicked on an ad for the advertiser’s

⁴ “Manage or Delete Your Location History.” Google Account Help. <https://support.google.com/accounts/answer/3118687?hl=en>.

⁵ “Popular Times, Wait Times, and Visit Duration.” Google My Business Help. <https://support.google.com/business/answer/6263531?hl=en>.

⁶ “Why You’re Seeing an Ad.” Google Ads Help. <https://support.google.com/ads/answer/7029660?hl=en>.

⁷ “About Customer Match.” Google AdWords Help. <https://support.google.com/adwords/answer/6379332?hl=en>.

⁸ Letter from Molinari, Susan (Google).

products or services.⁹ Google has expanded its use of Location History in advertising analytics since its introduction. In March 2017, Google announced that it had applied “deep learning models” to provide better accuracy for multi-story malls and dense geographies.¹⁰ Last October, Google announced that it will provide “impression-based store visits.” With the change, Google will provide advertisers with information on whether people visit stores just based on seeing the advertisement, even if they do not click it.¹¹

Google has also expanded the amount of information provided to advertisers, including the time taken for people to visit a store after clicking an ad, how many store visits come from repeat customers, and demographics on which groups are more likely to visit the store. In fact, Google’s response revealed, “Google uses location information in our ads products to infer **demographic information** [emphasis added], to improve the relevance of the ads users see, to measure ad performance, and to report aggregate statistics to advertisers.” We are particularly concerned about the use of location data for demographic inferences.

The power of this fine-grain, large-scale monitoring of the behaviors and movements of consumers is illustrated within Google’s regular blog posts about holiday shopping habits provided by the Location History data.¹² Google has an intimate understanding of personal lives as they watch their user’s seek the support of reproductive health services, engage in civic activities, or attend places of religious worship. All that it takes for users to expose themselves to this collection is to once allow an ambiguously described feature, for example when trying to display photos on a map on the Google Photo service, silently enabling the feature across devices with no expiration date. A feature that is only intended by a user to add city information to pictures is then opaquely used to precisely track people into stores for advertisers. Products like Store Visits and Customer Match bridge people’s online activities with their daily lives in ways that they are not fully informed of.

Most consumers do not understand the level, granularity, and reach of Google’s data collection, and there are serious questions about whether they have provided their informed consent and maintain a reasonable ability to avoid participating in this collection.

We are strong supporters of the FTC and its consumer protection mission. We have long advocated for robust enforcement where consumer harm is present. Congress empowered the FTC with a broad consumer enforcement mandate because it wanted the FTC to evolve with the marketplace. Today, data privacy and cybersecurity are two of the most important issues for consumers, and the loss of control over their personal data could have serious consequences for our economy.

⁹ “Measure More: Improving Estimated Total Conversions with Store Visit Insights.” Google Inside AdWords. December 18, 2014. <https://adwords.googleblog.com/2014/12/measure-more-improving-estimated-total.html>.

¹⁰ “New Measurement Innovations Unlock More Store Visits Data.” Google Inside AdWords. March 29, 2017. <https://adwords.googleblog.com/2017/03/new-measurement-innovations-unlock-more.html>.

¹¹ “Unwrapping New Innovations for the Holidays and Beyond.” Google Inside AdWords. October 24, 2017. <https://adwords.googleblog.com/2017/10/unwrapping-new-innovations-for-holidays.html>.

¹² “How Consumers Will Shop—and What They’ll Buy—This Holiday Season.” Google Inside AdWords. November 22, 2016. <https://adwords.googleblog.com/2016/11/how-consumers-will-shopand-what-theyll.html>.

We ask that you review Google's response, our attachments, and their privacy policies and open an investigation into the potential deceptive acts and practices used by Google to track and commoditize American consumers.

Sincerely,

Handwritten signatures of Richard Blumenthal and Edward J. Markey in cursive script.

RICHARD BLUMENTHAL
United States Senator

EDWARD J. MARKEY
United States Senator

Attachment 1

Letter from Senators Blumenthal and Markey, 1 Dec. 2018

RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES:

AGING

ARMED SERVICES

COMMERCE, SCIENCE, AND TRANSPORTATION

JUDICIARY

VETERANS' AFFAIRS

United States Senate

WASHINGTON, DC 20510

706 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
FAX: (202) 224-9673

90 STATE HOUSE SQUARE, TENTH FLOOR
HARTFORD, CT 06103
(860) 258-6940
FAX: (860) 258-6958

915 LAFAYETTE BOULEVARD, SUITE 304
BRIDGEPORT, CT 06604
(203) 330-0598
FAX: (203) 330-0608

<http://blumenthal.senate.gov>

December 1, 2017

Mr. Sundar Pichai
CEO
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai:

According to a concerning new investigation by the publication *Quartz*, Android devices are continually and covertly collecting users' location information and sending this information to Google – even when location services are disabled, the phone has been reset to factory condition, no apps are running or the SIM card is removed.¹ These practices, which Google confirmed in the article, are alarming, and the public deserves a full explanation from the company's CEO of the reason behind this data collection.

To date, Google's explanation for this location tracking behavior has been inadequate. As you know, the Federal Trade Commission has long considered it necessary to get affirmative opt-in consent before gathering consumer geolocation data due to the sensitive nature of that data. Furthermore, I am concerned you have not been candid with why this intrusive user tracking mechanism was implemented and to what extent Google is actually committed to ceasing collection of user location data.

As the Ranking Member of the Senate Commerce Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, a member of the Senate Judiciary Committee, and longtime advocate for consumer privacy protections, I respectfully request responses on the following questions:

- 1) Google's privacy policy asserts, "When you use Google services, we *may* [emphasis added] collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that *may* [emphasis added], for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers." Under what circumstances "may" Google collect this data? Under what circumstances does Google *always* collect this data? Under what circumstances does Google *never* collect this data? What do you mean by "when you use Google services?" Is *all* of Android's operating system a Google service? What do you specifically mean by "nearby devices?"

¹ Collins, Keith. Google collects Android users' locations even when location services are disabled." *Quartz*, 21 Nov. 2017. qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/.

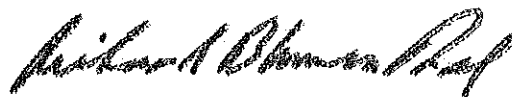
- 2) If a user goes "offline" and disconnects their mobile phone from the Internet for a period of time, or even places the device in so-called "airplane mode," does Google receive location data, Wi-Fi data, cell tower data, during this "offline" time period, even if location services is still on?
- 3) What location data does Google specifically collect from Android users and under what circumstances? Is the location data associated with a specific device ID? Is it associated with a specific user ID? Are there any other specific user or device identifiers involved? Can you please attach to your response examples of any relevant files or server logs transmitted by an Android device to Google so we can see for ourselves what location information is being compiled and transmitted?
- 4) Is a users' specific location data combined with other information Google collects about users' Internet activities? Is it combined with search data? DoubleClick cookie data? YouTube data, etc.?
- 5) Regarding "Wi-Fi access points," per your privacy policy, can you describe exactly what information is being collected and for what purpose? Are you collecting just known Wi-Fi access points a device has previously connected to or all Wi-Fi access points in range of the device? Are you collecting just network names or more information like a MAC ID, network address, signal strength or any other information? Are you collecting information about so-called "hot spots," other devices transmitting Wi-Fi signals? Are these Wi-Fi access points stored in a Google database and are they used for identifying a users' specific location?
- 6) Are there other network signals you are collecting, such as Bluetooth beacons? Again, all Bluetooth signals or only known or paired Bluetooth beacons? Specific device identifiers? Signal strengths?
- 7) As you know, today's mobile devices contain a range of sensors and consumers may or may not be fully informed about the purpose of those sensors. For example, consumers believe accelerometers are primarily for tracking a users' "steps" within a health app. Do you collect accelerometer data to assist in location tracking? How often and under what circumstances? Consumers believe barometer information is primarily used for "weather" within a weather app. Do you collect barometer information to assist in location tracking? How often and under what circumstances?
- 8) The Google spokesperson cited in the *Quartz* article stated that "we never incorporated Cell ID into our network sync system." Can you describe exactly what your network sync system is and what information is "incorporated" into it and for what purpose? Does the network sync system include other location-related information?
- 9) As you know, Google boasts to advertisers that it provides metrics on "store visit conversions" – meaning when a targeted ad translates into a retail store visit. These metrics are "calculated based on aggregated anonymized data from hundreds of millions

of Google users who opt-in to share Location History, click on a search or display ad, then visit a business location.”² How is Google able to obtain this data if, as was claimed by a Google spokesperson, location data was never used or stored? Specifically, how does Google know when a user visits a business location with “99% accuracy”? Has this location data ever been used to determine if consumers visited a retailer or was influenced by an online/mobile advertisement? If not location, has any other data been used to determine consumer behavior? How exactly are consumers “opting in” to this kind of tracking and use of their data to inform Google store visits conversions?

- 10) While you commit in the article to cease sending “cell-tower” location data to Google by the end of November, it is not clear if you are also committed to refraining from sending other forms of user location information – whether determined by GPS, Wi-Fi access points, nearby devices, sensors, or any other kind of technology? Can you clarify?
- 11) Does Google collect user data from Apple iOS devices through Google apps? If so, what data is collected from iOS devices? How is that data collected? Does Google recognize and respect all of the privacy choices made by iOS users? Is Google confident that it is not inadvertently collecting data from consumers who have affirmatively opted out of data collection or location sharing? For example, if a consumer is using Google maps on an Apple device, does Google receive and store that location information?
- 12) It would seem from the *Quartz* article and your privacy policy that a substantial *quantity* of data is transmitted to Google from Android devices and I assume that occurs on a regular basis. Who is paying for all of this location-related data transmission when a consumer is not using a specific app or not using the Internet? Is this location data transmitted over the cell network, where a consumer is paying for the data? Or just when a user is connected to Wi-Fi? How much information is being transmitted that is not related to a users’ specific app or Internet usage and is not for the purposes of diagnostics?

Thank you for your attention to these important questions. The American public is growing increasingly uneasy about the amount of data collected on them. It is important that they are fully aware of exactly when, how, and why their location information is being collected by the companies that they have put their trust in. I respectfully request a response by January 12, 2018.

Sincerely,



Richard Blumenthal
United States Senate

² Google AdWords. “Bridging the Customer Journey across the Physical and Digital Worlds.” *Google*. static.googleusercontent.com/media/www.google.com/en/us/adwords/start/marketing-goals/pdf/white-paper-bridging-the-customer-journey.pdf.

Attachment 2

Letter from Molinari, Susan (Google). Received by Senators Blumenthal and Markey, 12 Jan. 2018



January 12, 2018

The Honorable Richard Blumenthal
United States Senate
706 Hart Senate Office Building
Washington, D.C., 20510

The Honorable Edward J. Markey
United States Senate
255 Dirksen Senate Office Building
Washington, D.C., 20510

Dear Senator Blumenthal and Senator Markey,

Thank you for your letter of December 1, 2017. We appreciate the opportunity to explain our products and practices and to provide more information about the press report you note.

Privacy and security are critical issues for Google and we are deeply committed to keeping user data private and secure.

We want to be clear, the Quartz story you reference mischaracterizes what happened and how our systems work. The system it described did not use cell tower identifiers ("Cell ID") and never tracked user location. The Quartz article discussed device-side code that is part of a system Google uses to maintain a persistent connection between devices and servers so that the devices can receive notifications and messages in real-time. The system determines the optimal interval at which devices should "ping" servers so that this persistent connection stays open. If the connection closes, messages and notifications may be delayed and users would have to refresh their apps manually to get new messages. This system is designed to help users by determining the optimal ping interval, which helps preserve users' device batteries and makes real-time messaging available.

The claims that Google was using Cell ID from these transmissions to track user location are unfounded and untrue. While the device-side code transmitted data including Mobile Country Code or "MCC", Mobile Network Code or "MNC" and Cell ID, the server-side code (which would not have been accessible to the Quartz reporter) only logged MCC and MNC.

Although the Quartz article incorrectly stated that we were using Cell ID to track users' locations, we do use location data that we collect in other contexts to provide useful products and features to our users such as Google Maps. We welcome the opportunity to answer your additional

questions about how Google and Android work, and have included responses to these questions below.

1. **Google's privacy policy asserts, "When you use Google services, we *may* [emphasis added] collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that *may* [emphasis added], for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers." Under what circumstances "may" Google collect this data? Under what circumstances does Google *always* collect this data? Under what circumstances does Google *never* collect this data?**

We collect and use various types of location information in our products. The types of information we collect depend on a number of factors, including the service we are providing and the user's settings.

For example, standard Internet traffic information, such as IP address, can be used to provide the user with the correct language and locale for search queries. Some products, such as turn-by-turn navigation in Google Maps for mobile, use more precise location information such as GPS signals, device sensors, and Wi-Fi access points when the user has enabled device-based location services.

The Google Location Service (GLS) is the platform network location provider for most Android devices. GLS collects certain kinds of location information (such as Wi-Fi and GPS) from users who have opted into this service on their device and uses that information in an anonymized manner to help improve location accuracy and location-based services. This information also helps determine a device's location, which can be provided to applications that have the necessary location permissions. Users have the ability to opt into GLS when setting up their device or when using an application that uses GLS, and may subsequently disable this collection in their device's location settings at any time.

Location History is a different, Google account-level setting that allows users to store their location information with their Google account in order to get better results and recommendations across Google products. For example, users can see recommendations based on places they have visited with signed-in devices, or traffic predictions for their daily commute. Location History is off by default, and users must opt-in to turn on Location History for their Google account. Users have the ability to control their historical locations saved in their Location History, and can delete all or part of that history at any time.

- a. **What do you mean by "when you use Google services?" Is *all* of Android's operating system a Google service?**

Google plays two roles with respect to data collected on Android. First, Google develops and releases the Android operating system under an open source license, enabling anyone to

access the Android source code and create modified versions of it. In addition, Google develops proprietary mobile applications and services such as Google Play, Search, and Maps (referred to as "Google Mobile Services," or "GMS"), and licenses them separately from Android, meaning that device manufacturers can choose whether and on which devices to install GMS (or can use another mobile OS or suite of comparable apps). These apps, like those created by other developers, run on Android and make use of the platform and other device information to provide services directly to users. The Android operating system on devices with Google apps is a Google service covered by Google's Privacy Policy.

With respect to Android users, therefore, Google may receive information both from their use of Google apps, as well as Google applications installed on the device and services built into Android to make the platform and device function properly (such as the network sync system described below in question 8). Any personal information a user provides to Google, whether through Android system services or Google apps on Android, or that is otherwise generated and stored in a user's Google Account, is used and protected in accordance with the Google Privacy Policy.

This does not mean, however, that Google collects and uses all of the information on an Android device. For example, much of the information that a typical user generates while using Android is collected solely by third party apps running on the platform. As another example, Google enables device manufacturers to modify the open-source Android software such that Google does not receive any information from users of these devices. Information collected by other developers would be subject to their own privacy policies, rather than Google's.

b. What do you specifically mean by "nearby devices?"

With respect to your question on "nearby devices," many connected devices, such as Wi-Fi routers and Bluetooth-enabled devices, are able to detect and connect with each other. Application developers, including Google, may be able to infer a user's location through these connections. For example, if a user has opted into GLS, Google may use publicly broadcast Wi-Fi data from wireless access points in range of the device to help determine its location. As described in more detail below in response to question 5, only publicly broadcast Wi-Fi information is used to estimate the location of a device in this manner.

2. If a user goes "offline" and disconnects their mobile phone from the Internet for a period of time, or even places the device in so-called "airplane mode," does Google receive location data, Wi-Fi data, cell tower data, during this "offline" time period, even if location services is still on?

"Airplane" or "offline" mode is a common setting for mobile devices that disables the device's cellular antenna. When a device is switched into airplane mode, no cellular data, including cell tower data, is sent or received -- however, the device may contain information about the last cellular tower to which it was connected before airplane mode was enabled. A device's Wi-Fi

radio is typically controlled by a separate setting that can be enabled even when a device is in airplane or offline mode, for example to connect to an airplane's Wi-Fi network, or to use the device over a hotel's Wi-Fi network when a user is traveling somewhere without cellular service.

Accordingly, if a user enables airplane or offline mode but leaves on the Wi-Fi radio and connects to a Wi-Fi network, they will be able to continue to send and receive data on their device, including location data, over the Wi-Fi connection. This may include the types of location information described above, depending on the user's settings and the products or services they are using.

3. What location data does Google specifically collect from Android users and under what circumstances? Is the location data associated with a specific device ID? Is it associated with a specific user ID? Are there any other specific user or device identifiers involved?

As described above in our response to question 1, the types of location information that Google collects depends on a number of factors, including the service being used and a user's settings. With respect to Android specifically, location information can be used to provide a range of functionality, such as automatic traffic predictions or better search results. Depending on whether and how they want to use these features, users have a number of options for how their location data is collected, including the ability to turn location mode on or off for the device, as well as changing the device's "location accuracy" setting, which controls the sources used to estimate the device's location.

The information Google collects from Android devices for use in GLS is linked to a temporary and rotating device identifier that is not used by or shared with other services. It is not connected with any identifier that would associate that data with a specific user. If a user has opted into Location History, as described above, this location data is stored with their account identifier. Users can control the specific location information saved in their Location History, and can delete their history at any time.

a. Can you please attach to your response examples of any relevant files or server logs transmitted by an Android device to Google so we can see for ourselves what location information is being compiled and transmitted?

With respect to your request for examples of files or logs transmitted by an Android device, we are happy to organize a briefing to determine the specific information that might be most helpful to you.

4. Is a user's specific location data combined with other information Google collects about users' Internet activities? Is it combined with search data? DoubleClick cookie data? YouTube data, etc.?

We collect location information in many of our products, and use it along with other information to enhance and improve services for users, and do other things like detect fraud or improve security.

Google Search uses location data to make search results more relevant to the query and the user, and to select ads. For example, searches like "restaurants near me" depend on the device's location to understand what nearby means at that moment. Similarly, a word like "football" usually means something different in the U.S. than it does in the U.K. Some features on the search results page link to licensed content, and for that we try to link the user only to content available in her country. Finally, we use location to serve more relevant ads to that user, similar to the uses for organic search results.

As we describe in our [advertiser help center](#), Google's ad products may receive or infer information about a user's location from a variety of sources. For example, Google may use a user's IP address to identify their general location; receive precise location from a mobile device; or infer a user's location from search queries. In addition, websites or apps a user is using may send information about their location to us. Google uses location information in our ads products to infer demographic information, to improve the relevance of the ads users see, to measure ad performance, and to report aggregate statistics to advertisers. While our systems may use this information to show relevant ads, user location data is not shared with advertisers. For our ad services that operate on partner websites or apps, we may receive more precise location information in an ad request, but we use and store only the general area of the specified location.

YouTube uses a user's location to both personalize the user's watch and recommendations experience, to accurately serve the content licensed to YouTube by content providers, and to target ads. For instance, a user's country will determine what videos they see on the "Trending" tab of YouTube. The "Trending" tab is a set of videos that are rising in popularity in that user's country. For licensing restrictions, YouTube also allows many content owners to select which content is available in which countries. For example, when Disney changed the name of Zootopia to Zootropolis in the U.K., YouTube was able to serve the appropriate trailer to users in the U.K. Finally, as discussed above, YouTube uses a user's location to serve more relevant ads to that user.

Google may also collect and use location information to help detect fraud or other suspicious activity on a user's account. For example, users can review the dates and times on which their accounts have been accessed, as well as the IP address and general location from which these accesses occurred. This enables users to confirm their accounts have not been compromised when unusual activity -- such as an account access from a new country -- is detected.

5. Regarding "Wi-Fi access points," per your privacy policy, can you describe exactly what information is being collected and for what purpose? Are you collecting just known Wi-Fi access points a device has previously connected to or all Wi-Fi access

points in range of the device? Are you collecting just network names or more information like a MAC ID, network address, signal strength or any other information? Are you collecting information about so-called “hot spots,” other devices transmitting Wi-Fi signals? Are these Wi-Fi access points stored in a Google database and are they used for identifying a user’s specific location?

Questions 5(a)-(c) are describing the GLS we provide as a network location provider on Android devices, which uses sources like Wi-Fi and mobile networks to give location information faster and more accurately. When setting up their device or using apps or services that can use location services, a user may enable GLS to take advantage of these features. GLS uses publicly broadcast Wi-Fi data from wireless access points in range of the device to help determine its location. This may include any Wi-Fi access points in range of the device, and not just networks to which the device has previously connected.

These access points are stored and used to build models that estimate where each access point is located. This data is de-identified and only associated with a temporary, rotating device identifier, and no payload data/data packets are collected. As noted above, only publicly broadcast Wi-Fi information is used to estimate the location of a device.

To provide this functionality, Google collects MAC addresses, signal strength information, and radio channel information from these access points. Google also collects the name (also referred to as a “service set identifier” or “SSID”) associated with these networks, in order to identify and remove access points that network administrators have chosen to opt out of this collection through instructions provided by Google. SSIDs are discarded after being processed for this purpose.

6. Are there other network signals you are collecting, such as Bluetooth beacons? Again, all Bluetooth signals or only known or paired Bluetooth beacons? Specific device identifiers? Signal strengths?

The GLS described above does not use Bluetooth beacon information to determine location.

There are other Google products that may scan and collect certain information from Bluetooth beacons near the device. This includes information that any Bluetooth beacon may be publicly broadcasting for use, such as beacon type, beacon identifier, signal strength, and broadcast power. For example, if a user has turned on the opt-in Location History feature for their Google account, Google will use publicly available beacon information as one signal to help determine location. Other Google products, such as the Nearby service, use Bluetooth scanning to detect nearby Bluetooth beacons in order to show relevant notifications to users when they are near businesses, and other places that have installed Bluetooth beacons for this purpose.

7. As you know, today’s mobile devices contain a range of sensors and consumers may or may not be fully informed about the purpose of those sensors. For example,

consumers believe accelerometers are primarily for tracking a users' "steps" within a health app. Do you collect accelerometer data to assist in location tracking? How often and under what circumstances? Consumers believe barometer information is primarily used for "weather" within a weather app. Do you collect barometer information to assist in location tracking? How often and under what circumstances?

Many Android devices have built-in sensors that measure motion, orientation, and various environmental conditions. The Android operating system supports a number of these different sensor types, which vary from device to device. These sensors are used to provide a variety of functionality to application developers, such as the ability to measure device movement or positioning to support motion-based games, or to report a compass bearing for a travel application.

Android application developers, including Google, can use the accelerometer and barometer sensors, along with the gyrometer and magnetometer sensors, to more precisely determine a device's location. Google uses the accelerometer readings to help determining the device's orientation and direction, the gyrometer helps determine if a user is turning, and the barometer can help determine the user's elevation.

8. The Google spokesperson cited in the Quartz article stated that "we never incorporated Cell ID into our network sync system." Can you describe exactly what your network sync system is and what information is "incorporated" into it and for what purpose? Does the network sync system include other location-related information?

The network sync system supports real-time messaging in Google and third party applications on Android mobile devices (e.g., chat apps or notifications). Modern messaging and notification systems allow users to send and receive messages in real-time, so they do not have to "refresh" to see new messages. To do this, it is important for a device to keep its connection to servers alive for as long as possible. If the connection drops, messages will not arrive until the connection is re-established. And a device's battery power is drained when the device attempts to re-establish its connection to the server.

To keep this connection alive, Android devices and servers send pings to each other (referred to as "heartbeats"). If a device does not send a heartbeat ping after a certain period of time, the connection will terminate. For the benefit of users, Google seeks to determine the timing of these heartbeats that best balances the need to maintain a persistent connection between the device and the server with the preservation of device battery. If heartbeats are not frequent enough, connections are lost. If heartbeats are too frequent, battery power is depleted.

Mobile networks have different amounts of traffic and employ different technologies. These factors impact the optimal time interval to wait between each heartbeat. Thus, a device's mobile network provider will impact how frequently a device should send a heartbeat.

Knowing the network to which a device is connected helps Google determine how frequently a device should send a heartbeat ping. Google has access to mobile network information because the information that cell towers transmit to a device includes a MCC (indicating which country the tower is in), a MNC (indicating which cellular network operates the tower), as well as other information like a unique number assigned to each tower (Cell ID). In this instance, the device-side code on Android devices was designed to transmit information from the device that included all three of these data elements. The network sync system also relies on server-side code that determines what information Google actually logs on our servers in connection with the network sync system. This server-side code was written to only log MCC and MNC data for use in the network sync system. Once Google had the MCC and MNC from the device, we aggregated that information and used it to test different ping intervals per country and network in order to determine the optimal ping interval for each network and country.

This heartbeat “tuning” process was the sole reason Google collected the information transmitted by the device-side code at issue; this information was not used to determine user location. In fact, Google never used the Cell ID data from the transmissions to determine user location or, for that matter, ping intervals.

9. As you know, Google provides metrics on “store visit conversions” -- meaning when a targeted ad translates into a retail store visit. These metrics are “calculated based on aggregated anonymized data from hundreds of millions of Google users who opt-in to share Location History, click on a search or display ad, then visit a business location.” How is Google able to obtain this data if, as was claimed by a Google spokesperson, location data was never used or stored? Specifically, how does Google know when a user visits a business location with “99% accuracy”? Has this location data ever been used to determine if consumers visited a retailer or was influenced by an online/mobile advertisement? If not location, has any other data been used to determine consumer behavior? How exactly are consumers “opting in” to this kind of tracking and use of their data to inform Google store visits conversions?

As explained, Cell ID information was never used to track user location. It is completely unrelated to our Store Visits measurement feature. The Store Visits feature allows retail advertisers to get anonymized and aggregated reports of visits to their retail locations by Google users who also clicked on an ad for the advertiser’s products or services. Store visits are measured exclusively using data from Google users who have activated Location History, which provides a location timeline, stored against the user’s Google Account. Google correlates the observed store visits from those users who have activated Location History with those users’ ad clicks and then uses that data to estimate the aggregate number of store visits for all users who clicked on the advertiser’s ads.

Location History is turned off by default, meaning that users must opt-in to this service. Timeline

gives users full control over the locations they choose to keep. Users can pause or delete location history at any time via [Timeline](#).

We provide more information about Store Conversion services in our advertiser help center, which is available at: <https://support.google.com/adwords/answer/6361305?hl=en>.

10. While you commit in the article to cease sending “cell-tower” location data to Google by the end of November, it is not clear if you are also committed to refraining from sending other forms of user location information -- whether determined by GPS, Wi-Fi access points, nearby devices, sensors, or any other kind of technology? Can you clarify?

By the end of November 2017, Google deactivated the device-side code that transmitted the Cell ID to the network sync system, and that code was changed on each Android device the next time it checked in to receive updates.

As described in our previous answers, other forms of location data are collected and used by Google outside the network sync system, to provide a variety of product and service features.

11. Does Google collect user data from Apple iOS devices through Google apps? If so, what data is collected from iOS devices? How is that data collected? Does Google recognize and respect all of the privacy choices made by iOS users? Is Google confident that it is not inadvertently collecting data from consumers who have affirmatively opted out of data collection or location sharing? For example, if a consumer is using Google maps on an Apple device, does Google receive and store that location information?

Google provides a number of applications for iOS devices, which collect information consistent with Google’s Privacy Policy, user controls, and iOS platform rules and settings, including those pertaining to location data.

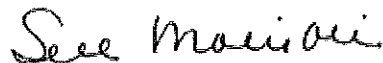
12. Does anyone pay for location-related data transmission when a consumer is not using a specific app or not using the Internet? If yes, please identify the parties. Is this location data transmitted over the cell network, where a consumer is paying for the data? Or just when a user is connected to Wi-Fi? How much information is being transmitted that is not related to a users’ specific app or Internet usage and is not for the purposes of diagnostics?

Data sent and received from Android devices may be transmitted over a Wi-Fi network or over the device’s cellular connection. In the case of mobile devices, any charges for transmission of data over a cellular connection -- including any location-related data -- would be governed by a user’s mobile carrier plan. The types and quantity of such data that a user’s device transmits would depend on the products or services they use, and, in some cases, a user’s settings.

Like all operating systems, Android collects diagnostic and other data from user devices to provide and improve system services and device functionality. As we describe above, one such function is the network sync system, which periodically exchanges pings between mobile devices and Google's servers. This helps to maintain a persistent connection so that the devices can send and receive notifications and messages in real-time without having to re-connect to Google's server and deplete battery power.

We appreciate the chance to clarify what happened and how our systems work, as well as explain Google's products and privacy practices. Protecting the privacy and security of our users is a top priority and we thank you for the opportunity to further underscore our commitments in these areas. Please let us know if we can address any other questions you might have or be a resource to you on our shared goals of improving users' mobile experiences and protecting users' privacy and security.

Sincerely,

A handwritten signature in cursive script that reads "Susan Molinari".

Susan Molinari
Vice President, Public Policy and Government Relations, Americas
Google

Attachment 3

Google Now Consent Process

Google Now (from Quartz)



Turn on this setting?

To get this feature, you need to have the following Google Account setting turned on for bob.tester01011970@gmail.com:

Places you go

Location History creates a private map of where you go with your logged-in devices

[LEARN MORE](#)

This setting allows Google to store and use information whenever you're signed in to a Google product (like Chrome or YouTube). By choosing "Continue", Google will turn this setting on for you. If you choose "Skip", your existing settings stay the same. You can manage your settings at any time in Google Settings.

SKIP

CONTINUE



Attachment 4

Google Assistance Consent Process

Google Assistant (from Quartz)



Give your new Assistant permission to help you

The Assistant depends on these settings in order to work correctly. Turn these settings on for:

gagtester01011970@gmail.com

 **Location History** ▼

Creates a private map of where you go with your signed-in devices

 **Device Information** ▼

Includes contacts, calendars, apps, music, battery life, sensor readings

 **Voice & Audio Activity** ▼

Records your voice/audio input to help recognize your voice and improve speech recognition

Please remember that the data governed by these settings may be saved from any of your signed-in devices. You can always control and review your activity at

