Google, Android and Location Tracking

September 2018

Executive Summary

Google voraciously collects all manner of user data from its various products and services, including highly sensitive location data, and it takes extraordinary steps to both enable and preserve its ability to collect this information. On Android, turning off all services that track location is a complicated endeavor, and keeping them off is even harder. However, even if a user is able to navigate through the maze of options to successfully turn off the location services Google permits to be turned off, Google still collects location information. For example, Google openly admits to collecting the Internet Protocol (IP) address of devices – regardless whether location is on or off – and Google makes clear that a user's IP address reveals a user's location.

By spreading location related settings across multiple screens and services, Google makes it extremely difficult to turn all location related services off. When setting up a new Android device, users must navigate an opaque, intentionally difficult, and time-consuming process to determine the impact of each location service setting, all of which require users to "opt out" as opposed to "opt in." Further, any effort to maintain their "opt out" location services status is frustrated by a constant prompting to turn location services back on.

This paper reviews the location preferences that Google disperses across different settings and the impact of user choices at account and device levels. Second, we detail how these various location services are not opt-in: each is enabled by default and therefore provides the greatest benefit to Google instead of enabling user privacy. Third the paper reviews how, despite user choices that appear to limit location tracking, Google still collects information that is used to determine user location.

1) How Google Collects Location Data

Google's Android operating system nests location controls under multiple different settings (Figure 1). In order to make informed decisions regarding which location services to enable, users must first understand the differences between these settings. Furthermore a user must understand which of these settings have account-level or device-level effect.

Account-level settings operate independently of device-level settings. When a consumer adjusts an account-level setting, the new setting applies to all devices where the user is logged into her Google account (including Gmail, Google Chrome, Google Maps, YouTube, etc.). Any device level setting change is limited to the specific item of hardware where the consumer made the adjustment.

	DESCRIPTION	OPT-IN / OPT-OUT	USER CHOICES
LOCATION SERVICES	"**Use Google's location service to help apps** determine your location. Anonymous location data will be sent to Google when your device is on."	Opt-Out	"YES, I'M IN" or "SKIP"
LOCATION ACCURACY	**Three Modes** - "High accuracy", "Battery saving", and "Device only." **Default setting:** "High accuracy use[s] GPS, Wi-Fi, Bluetooth, or cellular networks to determine location"	Opt-Out	Toggle icon (right and colored for on, left and gray for off). This setting not shown during Android set-up.
LOCATION SCANNING	"**Improve location accuracy** by allowing apps and services to scan for Wi-Fi and Bluetooth, even when those settings are off."	Opt-Out	Toggle icon (right and colored for on, left and gray for off).
LOCATION HISTORY	"[A]llows Google to store a history of your location data from all devices where you are logged into your Google Account and have enabled Location Reporting. Location History and Location Reporting data may be used by any Google app or service."	Opt-Out	"YES, I'M IN" or "NO THANKS" In the context of "Give your new Assistant permission to help you"

Figure 1: Four Android settings and services that relate to location information collection. [1]

Google Location Services

Google Location Services (GLS) operate at a device level and rely on sensors such as GPS, Wi-Fi, the cellular radio, and other technologies included in mobile devices to position a user in the world. If a user keeps the default settings prompted by Google, Location Services is enabled, Location Accuracy will be set to "High Accuracy" [2]and Location Scanning will be enabled for both Wi-Fi base stations and Bluetooth Beacons, regardless of a user's choice to turn Wi-Fi or Bluetooth on. The implications of user choices among the various Location Services settings are significant, but not intuitive, including:

- With Location Services turned on, Location Accuracy set to "Device only" and Location Scanning turned off, an Android device will only use GPS to provide the location of an Android device.
- When Location Accuracy is set to "High accuracy" and Location Scanning is enabled (the default setting for new device setup), an Android device will use sources including Wi-Fi, Bluetooth, and cellular radio to improve the accuracy of the device's position.

[1] Location Accuracy and Location Scanning are additional sub-settings that rely on Location Services. If Location Services is turned off, users are unable to access Location Accuracy and Location Scanning settings. "Descriptions" explained here are taken from Google's own descriptions and prompts.

[2] Phone will use GPS, Wi-Fi, Bluetooth, or mobile networks to determine location.

- If Location Accuracy is set for "High accuracy" and Location Scanning is enabled, the Android device will also scan for Wi-Fi and Bluetooth signals even if a user toggles Wi-Fi and Bluetooth off on the Android device.[3] Collected Wi-Fi base station and Bluetooth beacon data is transmitted to Google to provide updated data for GLS.

Google Location History
Location History tracks a consumer across all of the devices they may use (a smartphone, PC, laptop, tablet, smart television, etc.) when logged into their Google account, such as when using a Google web service like Gmail. When enabled, a user's location and various characteristics about a user's movements over time are recorded and transmitted to Google.

Google "Web & App Activity" Settings
In addition to specific location-labeled settings, Google also operates a service that collects user data via its "Web and App Activity" setting. During an Android device setup process, Google enables this account-level setting by default. With Web and App Activity tracking, Google combines user behavior on the web, such as searches, across multiple devices, so long as those devices are signed in using the same account. While not disclosed during initial Android device setup, Web and App Activity settings also track user location via IP address, and via activities such as searching for a location on Google Maps.

2) Google Location Services are Not "Opt-In"

GLS, as presented to a user on an Android device, is not "opt-in" but is instead "opt-out", and is both difficult to disable and to keep disabled. Google claims that "users have the ability to opt into GLS when setting up their device or when using an application that uses GLS."[4] In fact, users are required to "opt-out" during the setup of an Android phone - Figure 2 displays screenshots taken during the initial setup process of an Android device by a new user.

Critically, and in direct contradiction to Google claims that users "opt-in" to GLS, Figure 2 clearly shows all setup choices to share location information with Google are pre-configured to the "on" setting – the canonical definition of user "opt-out." Rather than being asked to accept these preselected options, users are prompted to click "next." By clicking through this series of screens a user has, by default, set up their Android device to enable the constant monitoring of their location using GPS, sensor data, and information about things near the device, such as Wi-Fi MAC address and Bluetooth beacons.[5]

[3] https://qz.com/1169760/phone-data/
[4] Google's response to Senators Blumenthal and Markey, page 2, paragraph 5
[5] https://policies.google.com/privacy#infocollect

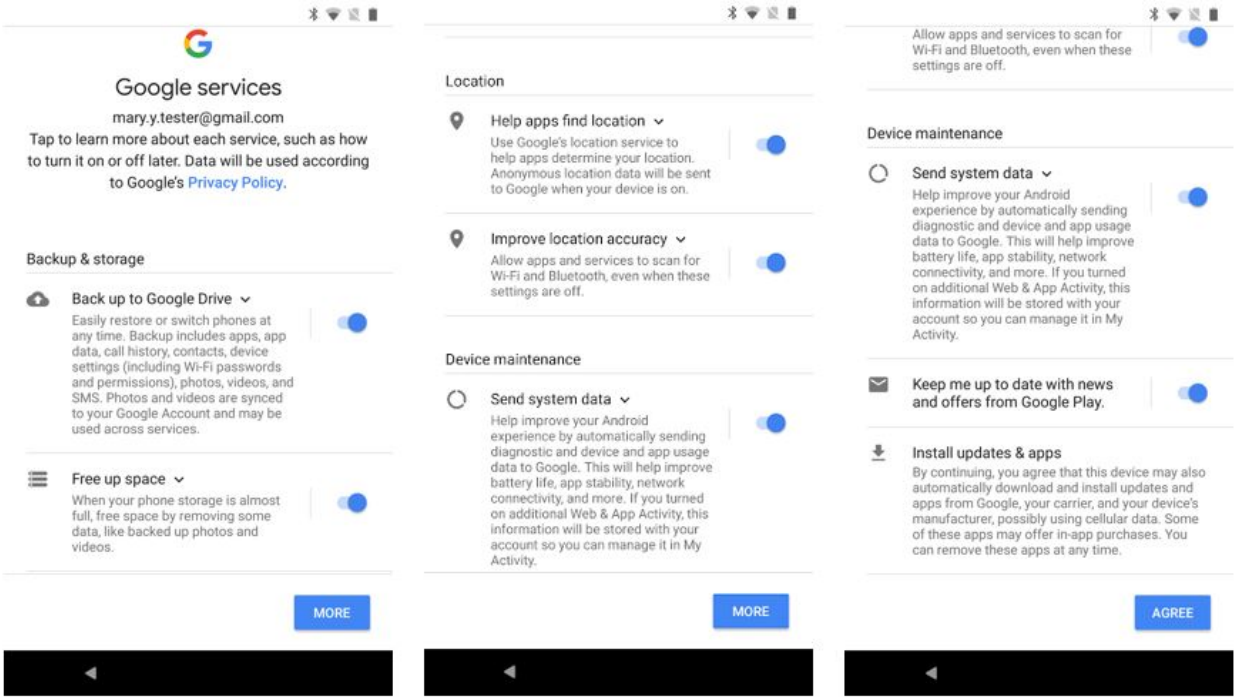


Figure 2: Google Services Defaults During Android Device Setup

Continuing through the Android smartphone setup process, users are prompted to enable **Google Assistant**[6] – a step that enables Location History, collection of device information, and recording of voice and audio activity of the user. Figure 3 displays the screenshots for setup of the Google Assistant service, bundling multiple settings with one "Yes I'm In". These default settings for Google Assistant also meet the criteria for an "opt-out" process, in direct conflict with Google's statement that "users must opt-in to this service."[7]

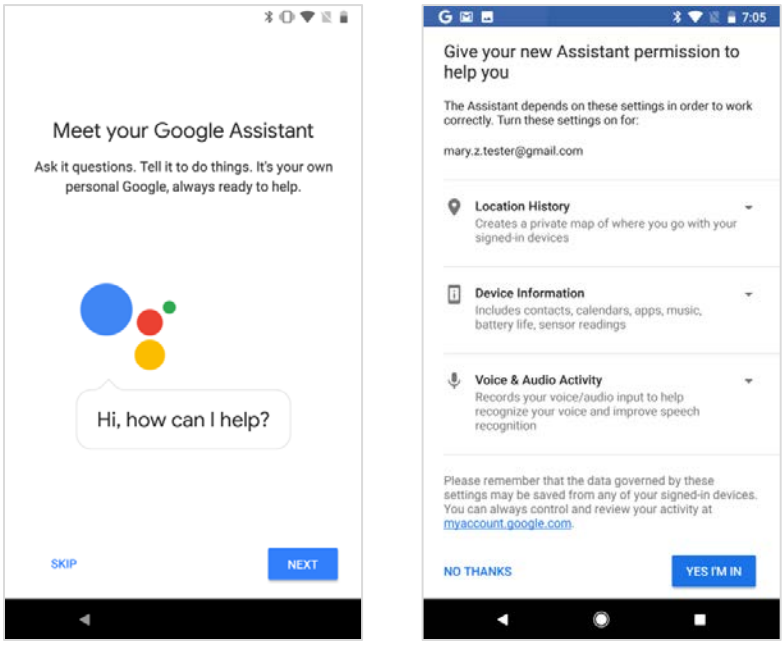


Figure 3: Google Assistant Setup Screens

[6] https://assistant.google.com

[7] Google's response to Senators Blumenthal and Markey, page 8, paragraph 5

After completing the setup process users can validate and control settings for device location via the Settings app and navigating to Google settings, then Location (Figure 4).

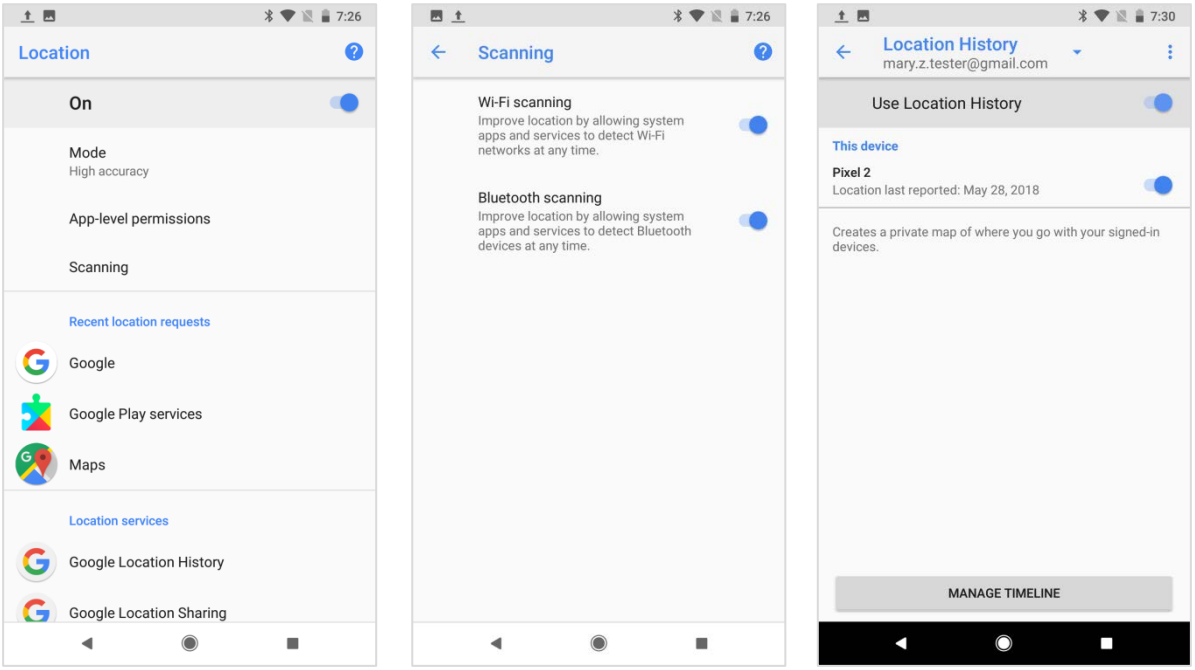


Figure 4: Location settings after Android device setup process

As demonstrated in Figure 4, if users accept Google's defaults during the setup process, the Android device is configured with Location Services enabled, Wi-Fi and Bluetooth scanning engaged, and Location History active.

Users can choose to disable GLS during the set-up process. However, if a user attempts to disable GLS, a warning dialogue box prompts an extreme scenario: "device location for all apps is turned off and you may not be able to locate your device if it is lost." (Figure 5) Note as well, the action prompt is to "Turn on Location" – reversing the user choice triggering the warning. Further, as described immediately below, many Google and third party apps will not function unless GLS is turned on. Therefore, Google forces user into an impossible ultimatum, have their every move constantly monitored, tracked, and stored or lose the functionality of their expensive smartphone.

If a user disables Location Services but then attempts to use a location aware app or service on their device, she will see the dialogue box shown in Figure 6. If the user clicks "OK" the service is enabled for the entire device and permanently, rather than enabling Location Services only for that particular app or service requesting the functionality.

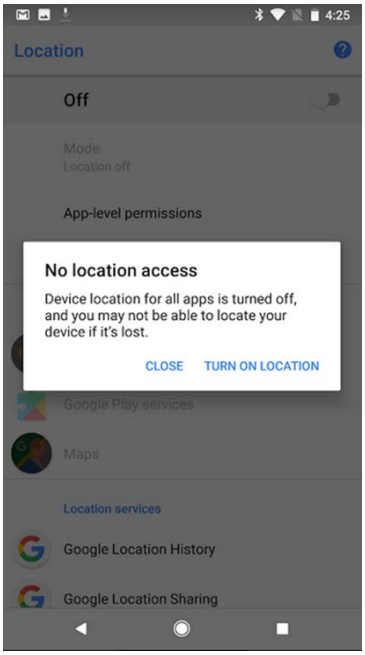


Figure 5: Location Services Warning

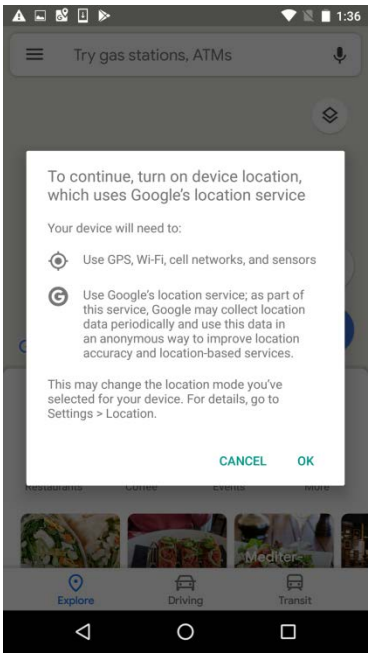


Figure 6: Re-Enable Location Services

Location History is treated in a similar manner by Google. Figure 7 highlights how the first time the Google Map app is launched, Google prompts the user to enable Location History if it is disabled. The user has two options, "Yes, I'm in" or "Skip," and they are informed that "Google needs to periodically store your location." It is worth noting that "Yes, I'm in" is highlighted by default and the "Skip" button blends in to the background of this screen. If the user selects the highlighted option, they have just turned on Location History universally across all devices associated with their Google account.

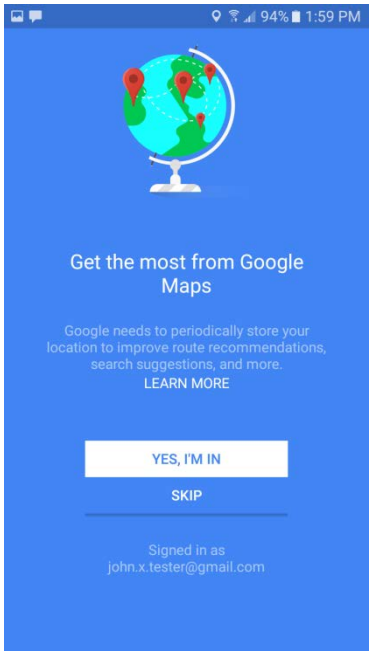


Figure 7: Location History Prompt

When adjusting the Location History setting, is it reasonable to expect that when Location History is disabled on one device, Google will not collect and store historical location on a user from that device. In practice, however, this is not the case. The Associated Press recently reported that Google in fact tracks historical locations of users who have Location History disabled on their smartphones. [8] This location tracking is a result of Google *also* tracking and storing user location across devices through its "Web and App Activity" settings. This setting is enabled by default to collect information across devices on an account (Figure 8).

[8] https://apnews.com/828aefab64d4411bac257a07c1af0ecb

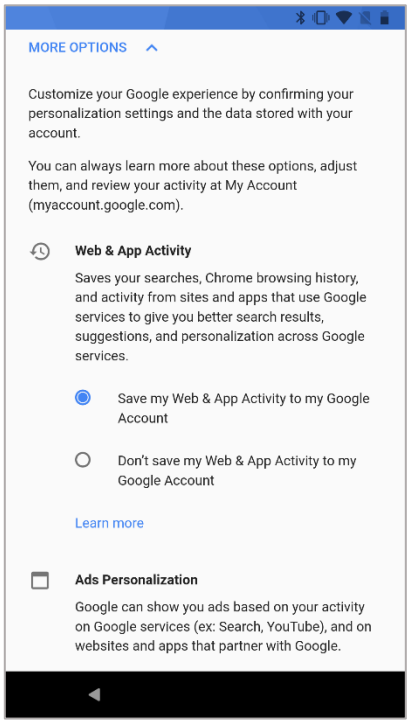


Figure 8: Web & Activity Setup Defaults

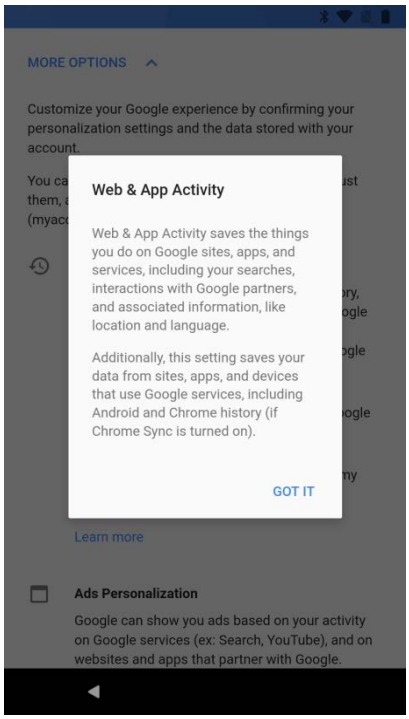


Figure 9: User Location Tracking Not Disclosed to User

Critically, the "Web & App Activity" setting does not disclose location tracking during the setup process, even if a user selects the "learn more" link (Figure 9). If the user has separate access to the internet and wishes to learn more than two sentences presented during setup about "Web & App Activity," they can review their Google Account Activity Controls and after digging through the site making three more navigation choices, they will learn what is saved as a result of enabling the setting (Figure 10). [9]

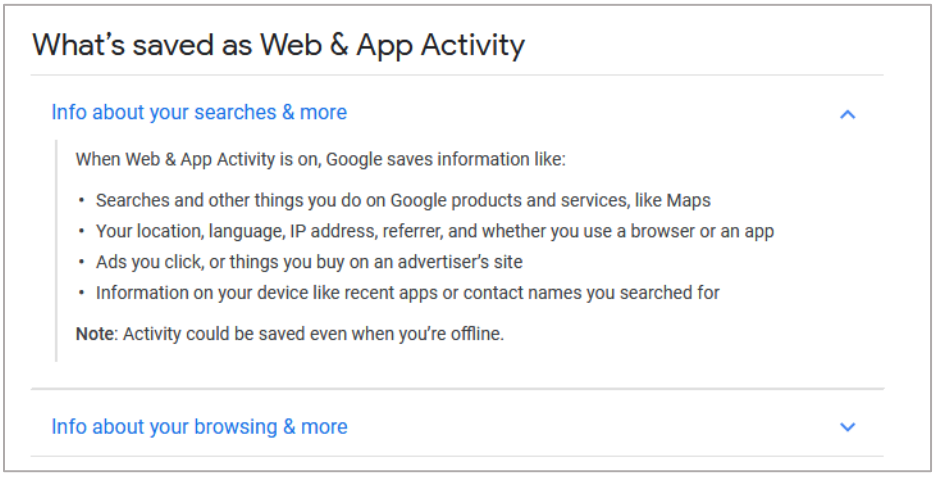
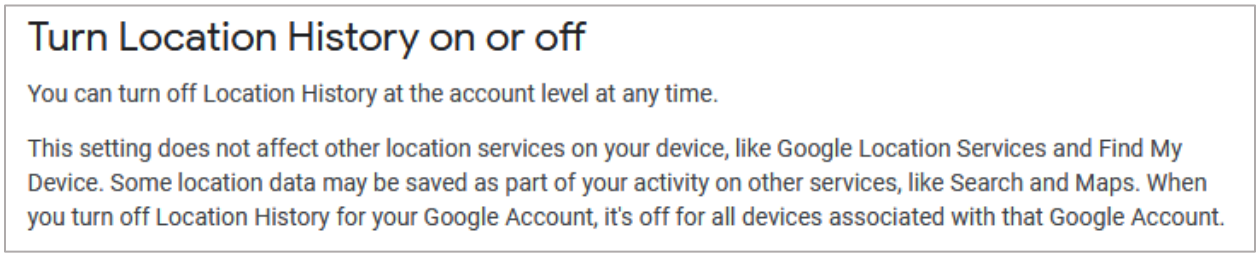


Figure 10: It takes multiple clicks to learn Google tracks your location with this setting.

[9] https://support.google.com/websearch/answer/54068?p=web_app_activity&co=GENIE.Platform%3DAndroid&oco=1

In response to an Associated Press report Google modified language detailing what happens when a consumer changes their Location History setting (Figure 11). Despite the first sentence claiming "You can turn off Location History at the account level at any time," Google goes on to disclose location data will continue to be collected and saved by Google. These statements are at best confusing, providing consumers with the illusion of control, while redefining the term "off" to mean "on."



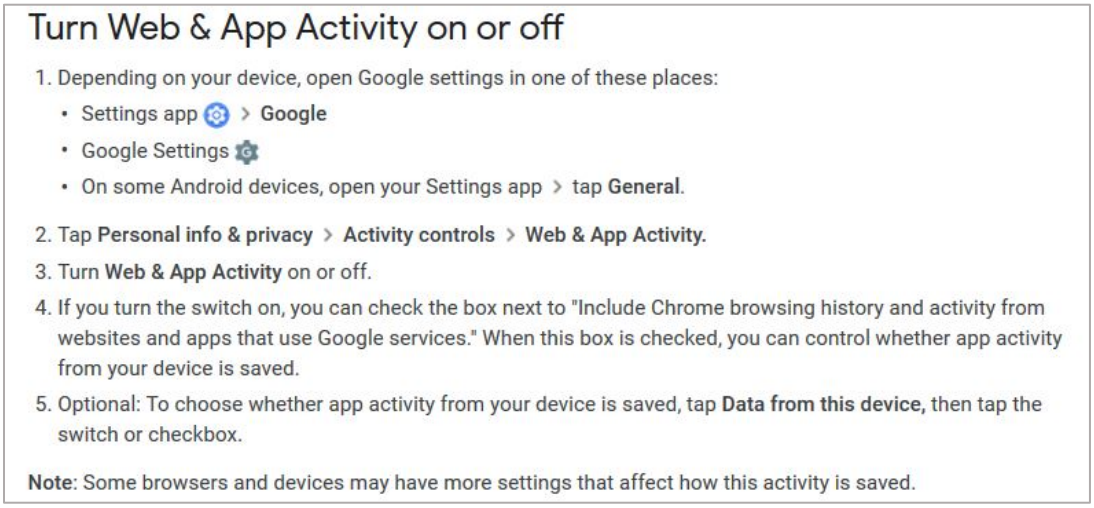
Turn Location History on or off

You can turn off Location History at the account level at any time.

This setting does not affect other location services on your device, like Google Location Services and Find My Device. Some location data may be saved as part of your activity on other services, like Search and Maps. When you turn off Location History for your Google Account, it's off for all devices associated with that Google Account.

Figure 11: Google's Updated Disclosure (after Associated Press report) [10]

According to Google, a user can turn "Web and App Activity" on or off by taking the following steps (Figure 12):



Turn Web & App Activity on or off

1. Depending on your device, open Google settings in one of these places:
   - Settings app > **Google**
   - Google Settings
   - On some Android devices, open your Settings app > tap **General**.
2. Tap **Personal info & privacy** > **Activity controls** > **Web & App Activity.**
3. Turn **Web & App Activity** on or off.
4. If you turn the switch on, you can check the box next to "Include Chrome browsing history and activity from websites and apps that use Google services." When this box is checked, you can control whether app activity from your device is saved.
5. Optional: To choose whether app activity from your device is saved, tap **Data from this device**, then tap the switch or checkbox.

Note: Some browsers and devices may have more settings that affect how this activity is saved.

Figure 12: Google's Instructions for Web & App Activity Control [11]

In contrast, the six screenshots of Figure 13 reflect the *actual* steps an Android user must take in order to change their "Web and App Activity" settings, which when enabled also track, store and send a user's location to Google. [12]

---

[10] https://support.google.com/accounts/answer/3118687?p=privpol_lochistory&visit_id=636703138939910406-3172221135&rd=1

[11] https://support.google.com/websearch/answer/54068?p=web_app_activity&hl=en&authuser=0&visit_id=636699552478272972-2174117461&rd=1&co=GENIE.Platform%3DAndroid&oco=1

[12] Screenshots taken on 16 August 2018 on an Google Pixel 2 running Android 8.1.0

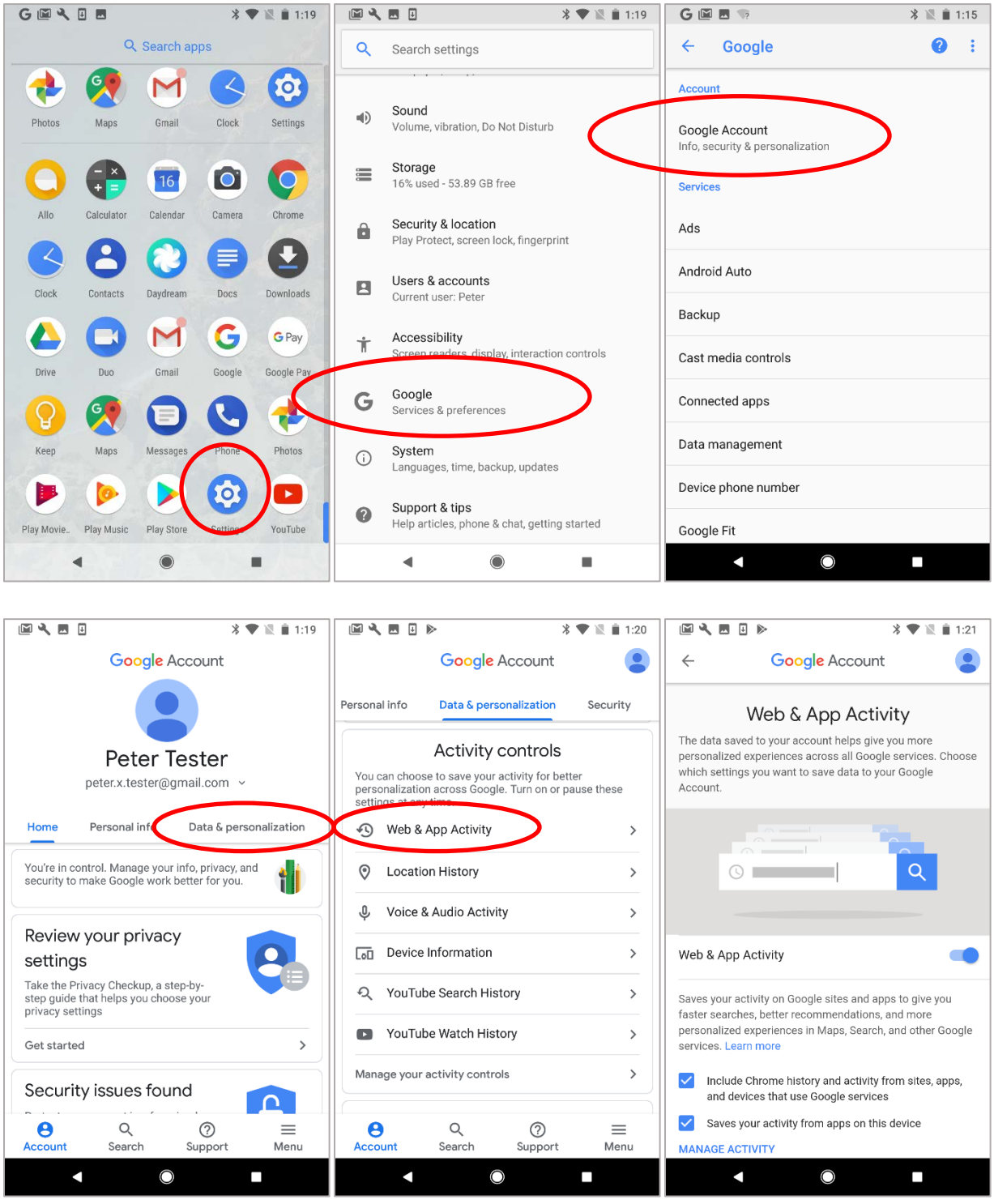


Figure 13: User steps to change Web and App Activity setting

3) Users are unable to turn off all location tracking on an Android device.

Google incorrectly claims that a user can turn off location tracking on an Android device. Even if a user is able to navigate through various opaque and intentionally difficult opt-out processes, they will be unable to prevent location tracking of their Android device. Irrespective of whether a user may toggle Google's Location Services on or off in the Settings app (Figure 4), Google continues to collect Internet Protocol (IP) addresses, which, according to Google's privacy policy[13], it uses to determine "the location from which a device is connecting to the internet." (Figure 14)

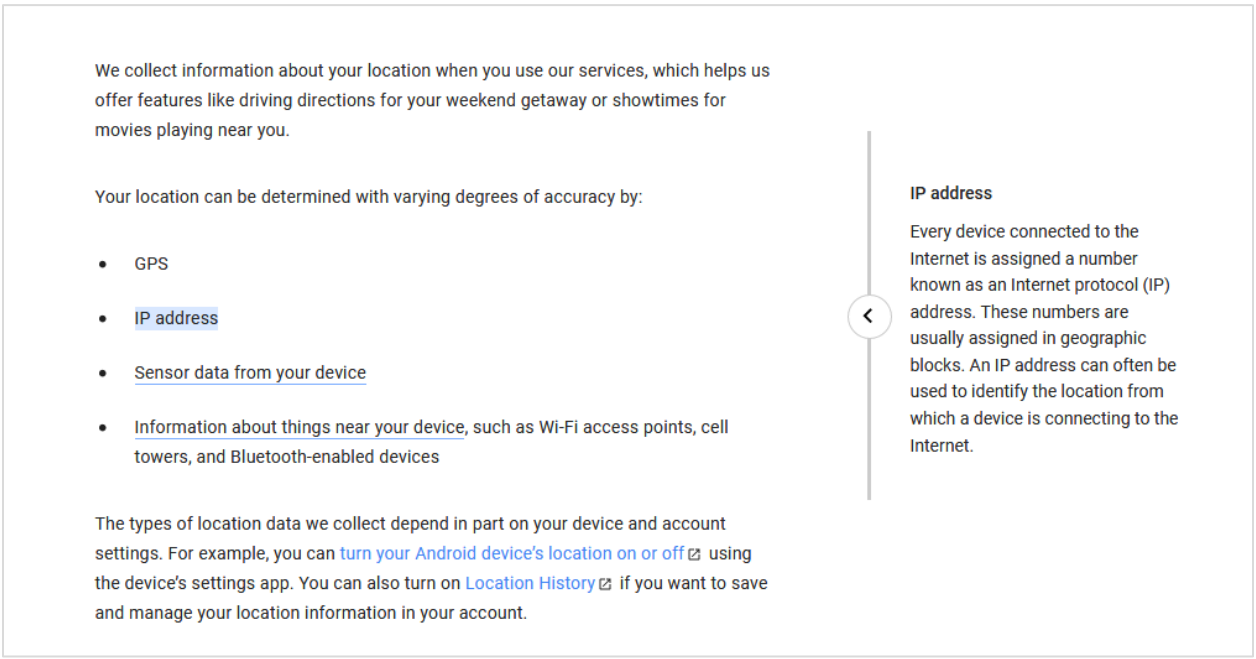


Figure 14: Portion of Google Privacy Policy Detailing IP Address Based Location Determination [14]

Google further confirms that it uses IP addresses to track a user's location through a disclosure made by Google's Vice President of Public Policy and Government Relations for the Americas, Susan Molinari in her letter to Senators Blumenthal and Markey (Appendix A). In that response, she states that Google continues to track consumer location for advertising through geolocation of IP addresses. She explicitly states, "We collect and use various types of location information in our products" [15] and then specifies that Google will "use a user's IP address to identify their general location." [16] This location data is then used by Google to target ads, as detailed in their own words: "Google uses location information in our ads products to infer demographic information, to improve the relevance of the ads users see, to measure ad

[13] https://policies.google.com/privacy/update
[14] https://policies.google.com/privacy#footnote-ip
[15] Google's response to Senators Blumenthal and Markey, page 2, paragraph 3
[16] Google's response to Senators Blumenthal and Markey, page 5, paragraph 3

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." [17]

Consumers are unable to control this behavior.

Android users are therefore unable to prevent the disclosure of their location to Google. Even if Google Location Services and Location History are disabled and they know enough to disable Web & App Activity settings, the IP address of Android devices will ***still*** be transmitted to Google. Again, Google notes that part of the operation of messaging and notification systems on Android, "it is important for a device to keep its connection alive for as long as possible", and as a result, "Android devices and servers send pings to each other (referred to as "heartbeats")." [18] These device "heartbeats" disclose the user's Android device IP address to Google independently of any location related user device settings. As such, Google can – and does - determine a user's location with Location Services disabled in order to target and sell ads.

Additional Consumer Activity Data Collected by Google

Google monetizes user data it collects for advertising purposes, [19] however, not all of the data sources Google collects are of equal value or sensitivity. Streams of user location and activity data from Android smartphones are uniquely valuable to Google, as they create detailed profiles of real-world behavior of individuals and their patterns of life. A second-by-second record of individuals every movement is highly sensitive, if not intimate, and permits Google to "close the loop," [20] tracking and targeting users with ads from the moment they wake and while they go about their daily routine.

Individuals are not likely to turn off location services Google pre-selects, as evidenced by the fact that nine in ten US smartphone owners use location-based services on their phone. [21] If an Android user does manage to opt-out (and continue to remain so), Google continues to collect a vast array of information about an individual's online activity [22] including:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services

[17] Google's response to Senators Blumenthal and Markey, page 5, paragraph 3
[18] Google's response to Senators Blumenthal and Markey, page 7, paragraph 5 and 6
[19] https://www.sec.gov/Archives/edgar/data/1652044/000165204418000027/goog10-qq22018.htm
[20] https://adwords.googleblog.com/2016/09/New-Digital-Innovations-to-Close-the-Loop-for-Advertisers.html
[21] http://totalaccess.emarketer.com/Reports/Viewer.aspx?R=2001793&ecid=MX1086
[22] https://policies.google.com/privacy#infocollect

- Chrome browsing history you've synced with your Google Account
- Telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls

This information is collected independently of location information.

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,

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