EVERY STEP YOU TAKE

How deceptive design lets Google track users 24/7

27.11.2018

FORBRUKERRÅDET

Table of contents

1 Summary

In this report, we look at how Google continuously tracks the location of its users through a number of different technologies. This tracking is implemented and enabled through the features “Location History” and “Web & App Activity”. These settings are integrated into all Google accounts as a personalisation feature, and are also used to facilitate targeted advertising.

We argue that consumers are deceived into being tracked when they use Google services. This happens through a variety of techniques, including withholding or hiding information, deceptive design practices, and bundling of services. We argue that these practices are unethical, and that they in our opinion are in breach of European data protection legislation because they fail to fulfill the conditions for lawful data processing.

2 Introduction

As smartphones have become ubiquitous consumer devices, connectivity is increasingly at our fingertips at all times. Through their combination of transmitters and sensors, our phones are able to sense their environment, and pinpoint our location as we carry them around. Where we move can reveal a lot about each of us, including our religious beliefs, political leanings, and sexual orientation. It is vital that digital service providers – who are omnipresent in our lives through our smartphones – treat location data about us with care, and only collect it when strictly necessary, with our consent.

The Norwegian Consumer Council is funded by the Norwegian Government, and is an interest organisation for consumers. Part of our work is to promote consumer rights such as privacy, security and balanced contracts in digital products and services. We have published reports on how smartphone apps fail to respect consumer rights,[1] how connected devices such as toys lack basic security and privacy-protective measures,[2] and how leading digital services use unethical design choices to steer users away from privacy.[3]

[1] “Threats to Consumers in Mobile Apps” https://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps/

[2] “Internet of Things” https://www.forbrukerradet.no/internet-of-things/

[3] “New analysis shows how Facebook and Google push users into sharing personal data” https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/

This report is part of our work on consumer privacy and the right to make informed choices. Through demonstrating how users are deceived into making privacy-intrusive choices, we argue that agency is being taken away from the consumer for the benefit of service-providers. We therefore urge service-providers to avoid using deceptive practices that undermine consumers' rights to make free and informed choices.

In our previous report "Deceived by Design", we looked at how digital service providers use different unethical design practices – referred to as "dark patterns" – to lead users into making certain choices. As part of this work, we briefly touched upon the confusing layout of Google's Location History setting. As a continuation of this work, we now look closer at how Google tracks the location of their users.

Chapter 3 provides background on Google and the Android operating system, location tracking in general, and on the concept of dark patterns. In chapter 4, we identify some of the problematic practices that consumers are exposed to when setting up an Android device and creating a Google account. A legal analysis of Google's practices in light of the General Data Protection Regulation (GDPR) is included in chapter 5.

2.1 Method

In this report, we look at how several Google services collect location data from smartphone users, demonstrated through user testing. Most of the tests were performed using an Android device, with a few tests performed on an iPhone for reference. This was done through what we consider a regular user experience. When setting up a new Android device, users typically go through a process of registering and/or logging in to a Google account, and adjusting or accepting a number of settings related to data collection, such as voice data, location data, and diagnostic data. The testers documented every click and choice that appeared during the process of setting up the device, registering a new Google account, and launching the preinstalled Google apps for the first time.

The analysis and discussion throughout the report is based on European data protection legislation and ethical principles from literature on user interface

design.[4] These principles serve as benchmarks used to consider the legal and ethical aspects of the design and content of the process.

The tests in chapter 4 were performed in July 2018 using a Samsung Galaxy S7 Android device running Android version 8.0.0, which had been reset to factory settings. The results were reproduced in October 2018 on the same Samsung device, and on a Google Pixel device running Android version 9.[5] Although the settings and device setup process may vary somewhat between devices, we regard the Google account setup can to be representative of a typical user experience. The screenshots were taken in July and August 2018. A diagram that illustrates how users can turn off or avoid location tracking is included as an appendix.

Because this is an analysis of digital settings and content that may be subject to change, we cannot say with certainty that all users of these services have been presented with identical settings and design patterns during the setup process. However, our opinion is that the findings are and will continue to be relevant even if changes are made, because these examples illustrate the challenges consumers face in digital services at a given point in time.

This report was written with funding from the Norwegian Research Council through the ALerT research project[6] and the Norwegian ministry for Children and Equality. We are also thankful for invaluable help and input from the European consumer organization BEUC, the Dutch consumer organization Consumentenbond, None of Your Business (noyb), Jon Worth, Dr. Frederik Zuiderveen Borgesius, and Privacy International.

3 Background

The smartphone market is generally split between two operating systems (OS), Apple's iOS and Google's Android OS. Apple's iOS is used on all iPhone and iPad devices, while the majority of other smartphones and tablets run on a version

[4] See "Nudges for Privacy and Security", https://dl.acm.org/citation.cfm?id=3054926 and "Dark patterns and the ethics of design" https://medium.com/adventures-in-ux-design/dark-patterns-and-the-ethics-of-design-31853436176b

[5] Testers found minor differences between the Samsung Galaxy and the Pixel device, but not significant enough to change the conclusions in this report.

[6] "ALerT - Awareness Learning Tools for Data Sharing Everywhere" https://www.nr.no/en/projects/alert-awareness-learning-tools-data-sharing-everywhere

of Android. Although Apple's iOS is also popular among consumers, we have chosen mainly to focus on Google apps and Android for several reasons. These reasons are explained below, together with relevant background information.

3.1 Business model

Google and Apple have somewhat different business models.[7] Apple is primarily a hardware provider, with revenue coming from selling devices such as iPhones, with additional revenue coming from their App Store. Google makes a significant part of their revenue from data-driven advertising.[8] In 2017, Google was rated the most valuable brand in the world, with a brand value of $109.5bn /€95bn.[9]

Google is a subsidiary of Alphabet Inc., and deliver a vast amount of consumer- and business-facing services. These consumer-facing services include, but are not limited to, Google Search, Google Maps, Gmail, Android, YouTube, and Google Assistant. Google also runs a large number of business facing services, including analytics and advertising services.

Google provides most of its consumer-facing services at no direct financial cost to the user. Rather than having users pay an upfront fee for using these services, Google collects data about its users and their behavior, which is monetized through advertising and other business-facing services. Through its various services, Google collects a comprehensive picture of its users, including device information, browsing history, precise geolocation, and more. On Android devices, a large amount of data is collected passively in the background without any active actions from the user.[10]

Through compiling profiles about individual users, as well as user segments or categories based on preferences or behavior, Google can offer advertisers numerous ways to reach a target audience. Advertisers can use Google's ad

---

[7] "How Do Tech Companies Make Money? Visualizing Tech Giants Business Models" https://fourweekmba.com/tech-giants-business-models/

[8] "Once again, Alphabet made a lot of money on Google advertising and this time Wall Street is thrilled" https://qz.com/970765/alphabet-goog-q1-2017-earnings/

[9] "The world's most valuable brands revealed" https://www.independent.co.uk/news/business/news/worlds-most-valuable-brands-facebook-google-apple-amazon-a7556571.html

[10] A 2018 study showed that an idle Android device communicated with Google servers more than ten times as often as an idle iOS device communicated with Apple servers. "Google Data Collection research" https://digitalcontentnext.org/blog/2018/08/21/google-data-collection-research/

services to reach particular audiences with tailored ads, often called "programmatic advertising". Continued data collection about how users respond to ads, and tracking of individual users across different devices, enables Google to offer advertising spaces that are tailored to the individual user, and that are delivered "in the right moment with the right message".[11]

3.2 Market share

The Android OS is by far the dominant international market player, with an estimated 85 % of the global mobile OS market share.[12] Android is used by a variety of smartphone providers, including Samsung, Huawei, Sony, and more. Users of these phones may not be aware that Android is a Google product, and therefore that they are using a Google-powered device. Apple's iOS, on the other hand, has a market share between 10 % and 15 % globally. iOS is only available on Apple products such as iPhones, meaning that users who are using iOS already have a customer relationship with Apple.

3.3 Android and competition

Android-users have to create a Google Account before they can access the Google Play app store, which is required to download new apps, or to receive app updates. Additionally, when setting up an Android device for the first time, users have to agree to Google's privacy policy, and terms and conditions. This entails that users have to agree to Google processing user data collected through the Android device, such as device ID, usage data, and location data.

Google provides the Android OS through an open source license, meaning that the smartphone manufacturer does not have to pay Google for using or adapting Android (to develop so-called Android forks). However, the Android license agreement for manufacturers comes with a number of caveats.

While the Android OS is distributed under an open source license, the suite of apps called Google Play Services is proprietary software.[13] In order to use the Android OS on the phones they manufacture, phone manufacturers are required to include the Google Search and Google's Chrome browser

[11] "Organize audience insights" https://www.thinkwithgoogle.com/marketing-resources/programmatic/organize-audience-insights-programmatic-buying/

[12] "Smartphone OS market share" https://www.idc.com/promo/smartphone-market-share/os

[13] This includes services such as Google Play, Gmail, Google Maps, and more. "Google's Iron Grip On Android" https://arstechnica.com/gadgets/2013/10/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/

preinstalled on the phones, and use Google Search as a default search engine as a condition to use Google's proprietary apps.[14]

If, for example, Samsung were to choose not to include Google Chrome on their phones, they would be barred from including the Google Play app store. Without Google Play, users will be unable to receive app updates or install other apps on the phone without going to third party app stores.[15] Additionally, if for example Samsung were to release a phone with a competing OS on it, they would lose access to use Android on all their other phone models. In July 2018, Google was fined by EU antitrust authorities for abuse of market dominance because of these practices.[16]

3.4 Operating system functionality

Although many Google features and services are available also for iPhone users, the implementation is different between the two operating systems. Since iPhones do not come with any preinstalled Google apps, users have to actively download and activate any Google services they may want to use.[17] This also means that iPhone users do not need to have a Google account in order to download other apps.

Additionally, the app permission systems of Android and iOS are different. For example, both operating systems will ask users whether they want certain apps to access location data. However, on Android, allowing any particular app to access location data will allow the service to collect this information in the background, not just while the app is actively in use. On iPhones, users launching an app that requests location data are asked whether they want to give the app access to location at all times, or "only while using the app".[18] In other words, iPhone users can choose to give a map service access to location

[14] "EU says Google abuses its Android dominance" https://www.cnet.com/news/eu-hits-google-with-android-app-abuse-charges/

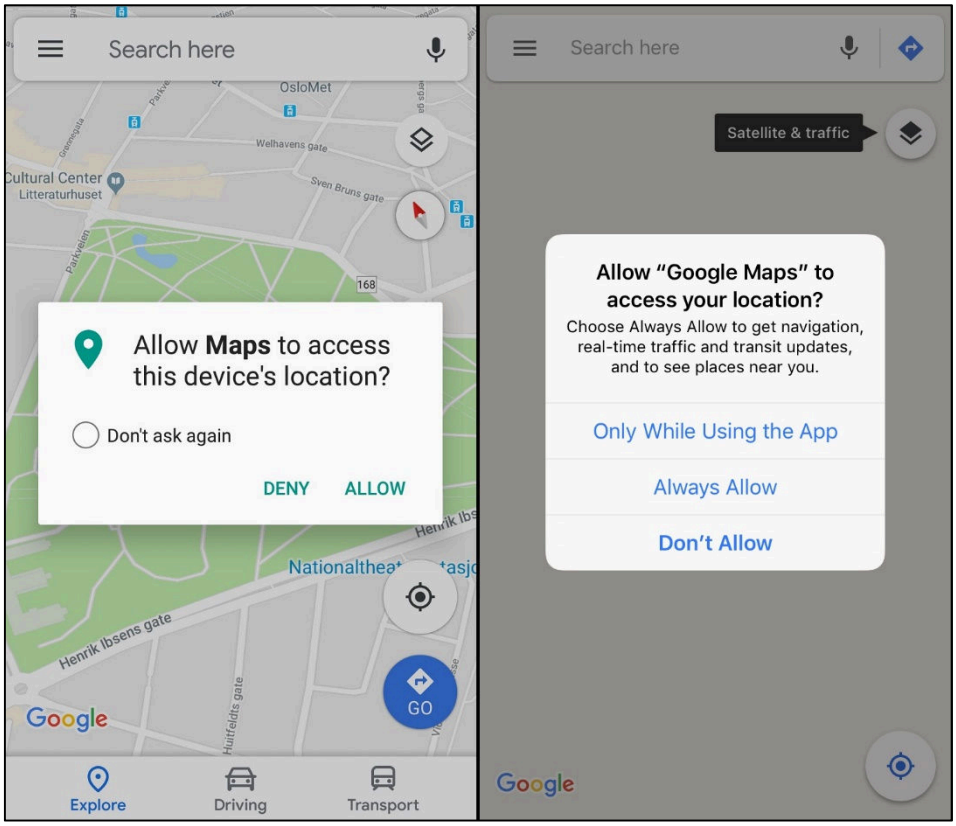
[15] "New Android OEM Licensing Terms Leak" https://arstechnica.com/gadgets/2014/02/new-android-oem-licensing-terms-leak-open-comes-with-restrictions/

[16] "Google fined £3.8bn by EU over Android antitrust violations" https://www.theguardian.com/business/2018/jul/18/google-faces-record-multibillion-fine-from-eu-over-android

[17] Except Google Search, which is set as the default search engine on iPhones. Google reportedly pays Apple between $9 and $12 billion for this. http://fortune.com/2018/09/29/google-apple-safari-search-engine/

[18] "Uber users on iPhones can now block the app from always tracking their location, thanks to Apple's new iOS update" https://nordic.businessinsider.com/thanks-to-ios-11-users-can-stop-uber-from-tracking-them-24-7-2017-9

only when they are actively using the app, while on Android users have to choose between either letting the app access location services at all times, or completely block the app from accessing location.



1 Google Maps permissions prompt. Android on the left, iPhone on the right.

3.5 Location tracking

Location data can be described as a physical position point, defined by geographical coordinates. Location tracking means that the location of a person or entity is recorded over time. When aggregated, location data can also reveal broader patterns or anomalies. As we use our smartphones for an increasing number of tasks in our everyday lives, the usefulness of location tracking is obvious. Interactive real-time maps, searches that show nearby businesses, and weather services are perhaps the most obvious examples, but location tracking can also be aggregated and used for route planning, traffic management, and so on.

It is possible to infer a lot about an individual based on their location history. Studies have demonstrated that four approximate location points is often

enough to accurately identify an individual.[19] Inferences about sensitive personal data can also be made from tracking your location. For example religious views (spends time in a mosque), political stance (attended a protest march), and health related issues (visits a cancer treatment center).

Furthermore, information about your whereabouts can reveal your habits and your personality. This can be used to target advertising, or for individualised offers and services. If you frequent a pub, indicating a drinking habit, this could be valuable information for an insurance company. Similarly, someone who regularly goes for runs could be offered lowered premiums, or be targeted by advertisements for sporting equipment. Consumers may be subjected to discriminatory practices through the individualisation of messages and offers, although these forms of discrimination can be difficult to discover.[20]

Companies such as Google are not collecting location data in a vacuum. Geolocation is part of a bigger picture, and can be combined with other data such as browsing history, preferences, social networks, shopping history, and so on. For example, information about visiting a physical store can be used to measure ad effectiveness, as long as the person who saw the ad can be identified as the same person who visited the store. This practice of combining tracking data to draw new inferences is also called "closing the loop".[21]

Consumer studies have demonstrated that consumers are particularly conscious and worried about the tracking of their location. An international 2018 study that asked more than 8000 consumers about location data and privacy, showed that 75-80 % of consumers feel vulnerable when their location data is being shared.[22] Despite this general anxiety, many consumers feel powerless to limit the amounts of data being collected through their smartphones. Consumers are also generally unlikely to adjust the privacy settings of the services they use, which makes it crucial that service-providers act responsibly when it comes to the types of data they collect, when they collect it, and how they use it.

---

[19] "Study shows how easy it is to determine someone's identity with cell phone data" https://phys.org/news/2013-03-easy-identity-cell.html

[20] In 2015, researchers at Carnegie Mellon University found that Google's advertising platform was showing higher paying jobs to more men than women. "Google's algorithms advertise higher paying jobs to more men than women" https://www.theverge.com/2015/7/7/8905037/google-ad-discrimination-adfisher

[21] "New digital innovations to close the loop for advertisers" https://adwords.googleblog.com/2016/09/New-Digital-Innovations-to-Close-the-Loop-for-Advertisers.html

[22] "Privacy and Location Data: Global Consumer Study March 2018" https://www.here.com/en/node/40306

3.6 Dark patterns and deception

As we use digital services, we are subtly being influenced in various ways, including through the user design of the service. These can be innocuous nudges, such as giving us easy access to relevant information, but some of these practices have a more insidious motive. Through so-called "dark patterns", deceptive design practices, users are nudged toward making choices that are in favor of the service-provider, and often against their own interests.[23]

Dark patterns come in many shapes, and encapsulate many different design practices. For example, the use of color, visibility and wording may serve to steer users toward choices that benefit the service provider. This can include misrepresenting the consequences of a choice, by only focusing on certain aspects that put the service provider's preferred choice in a positive light. Similarly, information that might dissuade the user from opting in to a service can be withheld or hidden from view, giving users a skewed impression.

As many mobile phone services are used on the go, users will often take the path of least resistance in order to access a service as soon as possible. Making the least privacy friendly choice part of the natural flow of a service, can be a particularly effective dark pattern when the user is in a rush, or just wants to start using the service. For example, this can be done by using a certain click-flow,[24] then subverting the design mid-flow by switching the expected function of a button. When setting up an Android device, the "Continue" button is always a blue button placed in the right corner. However, for some steps of the process, the blue button also entails enabling extra features.[25] If users are not paying full attention every step of the way, they may end up unintentionally enabling a setting without knowing that they have done so.

Furthermore, users can be deceived by being discouraged from making an active choice, paving the way for default settings that disfavor the user. When users are asked to opt out of certain settings, rather than opting in, the service-provider could be exploiting the users' disposition to leave the default settings enabled.[26] Similarly, continuous prompts that ask users to enable settings do

[23] "Dark Patterns are designed to trick you (and they're all over the Web)" https://arstechnica.com/information-technology/2016/07/dark-patterns-are-designed-to-trick-you-and-theyre-all-over-the-web/

[24] A pattern of buttons or links that have to be clicked in order to proceed through a process.

[25] See chapter 4.5.3

[26] "Do users change their settings?" https://www.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/

not respect the users' original choices, and may wear out the users and make them resign to clicking "I accept" despite originally being reluctant.

Another dark pattern entails service providers "bundling" different services that are not functionally interdependent. For example, using a map service could be made contingent on uploading your web browser history. Such bundling can make users share information that they otherwise would not, because the alternative is punishment in the form of being denied access to a service or function.

Dark patterns are often considered unethical design practices.[27] The use of deceptive design tricks to obfuscate important information, bundling, and misrepresenting what settings actually do, are also at odds with the notion of giving users agency to make informed choices. As such, dark patterns have the potential to be used in ways that circumvent laws meant to protect consumers.

4. Google and location tracking

Google mainly tracks user location through two settings, Location History and Web & App Activity, which are both integrated into the Google user account.[28] These settings can be controlled through the Google account or through Android settings, and collect and combine data from other Google Services that collect user data, such as Google Maps, YouTube, Google Chrome, and Google Photos.

In this chapter, we first give a brief overview of the Location History and Web & App Activity settings. Subsequently, we look at how these settings are presented to the user in different contexts. This is followed by a discussion of the different practices that mislead users throughout the process.

4.1 Location History

Location History is a Google account setting that continuously logs the location of the user. According to Google, the Location History feature *"helps you get better results and recommendations on Google products. For example, you can see recommendations based on places you've visited with signed-in devices, or*

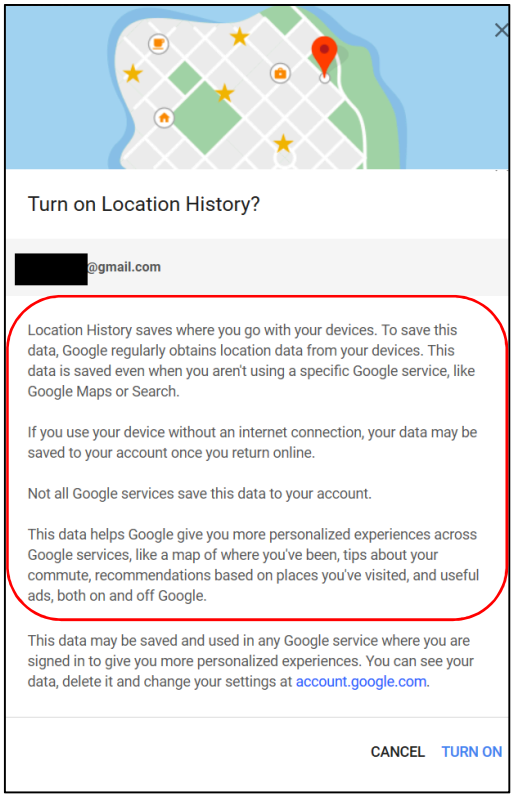
[27] "Dark patterns and the ethics of design" https://medium.com/adventures-in-ux-design/dark-patterns-and-the-ethics-of-design-31853436176b

[28] The Google user account is the main hub for most Google services, and is used to log in to Android, Gmail, Search, YouTube, and much more.

traffic predictions for your daily commute."[29] The location data collected through Location History is derived from GPS, Wi-Fi scanning, and Bluetooth scanning, which means that Google can track a user's precise location inside buildings as well as outside.

According to the description on Google's My Account website, data collected through Location History is also used to serve targeted advertising:

> *"This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google."*[30]



2 Google Location History, as seen on a Google Account.

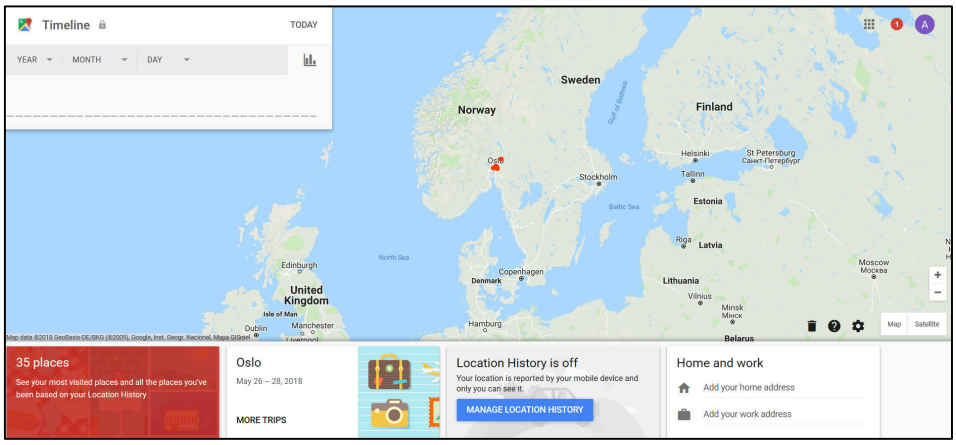
When enabled, Location History collects a variety of user data, including mode of transportation (walking, driving, on a tram, entering a vehicle, etc.), barometric pressure (altitude), Wi-Fi information, GPS coordinates, and the battery level of your device. This data is transmitted to Google, and stored as a part of the user's Google account.

---

[29] "Google Account Help - Manage or delete your Location History" https://support.google.com/accounts/answer/3118687?hl=en

[30] "Google Activity Controls" https://myaccount.google.com/activitycontrols

Some of the information inferred through this data collection (location, route, mode of transportation, which shop you visited at what time) is available on the user account ("Location History Timeline"), where users can look through their movement history for the period the feature has been enabled.[31] Other data, such as barometric pressure, nearby Wi-Fi hotspots and Bluetooth beacons, and battery level, is not visible to the user, but is collected passively in the background.



3 Google Timeline on a web browser on a PC.

According to Google, the Location History feature is voluntary, and users must opt in before the feature starts tracking user location.[32]

4.2 Web & App Activity

Web & App Activity is another Google account setting, which collects a variety of user data from an assortment of Google services. As shown in the screenshot below, Web & App Activity is described as *"Saves your searches, Chrome browsing history and activity from sites and apps that use Google services. This gives you better search results, suggestions and personalisation across Google services"*.

Google users can look at the data collected through Web & App Activity through the "My Activity" timeline on their profile, which is logged separately from the Location History Timeline.[33] This log includes timestamped records of which

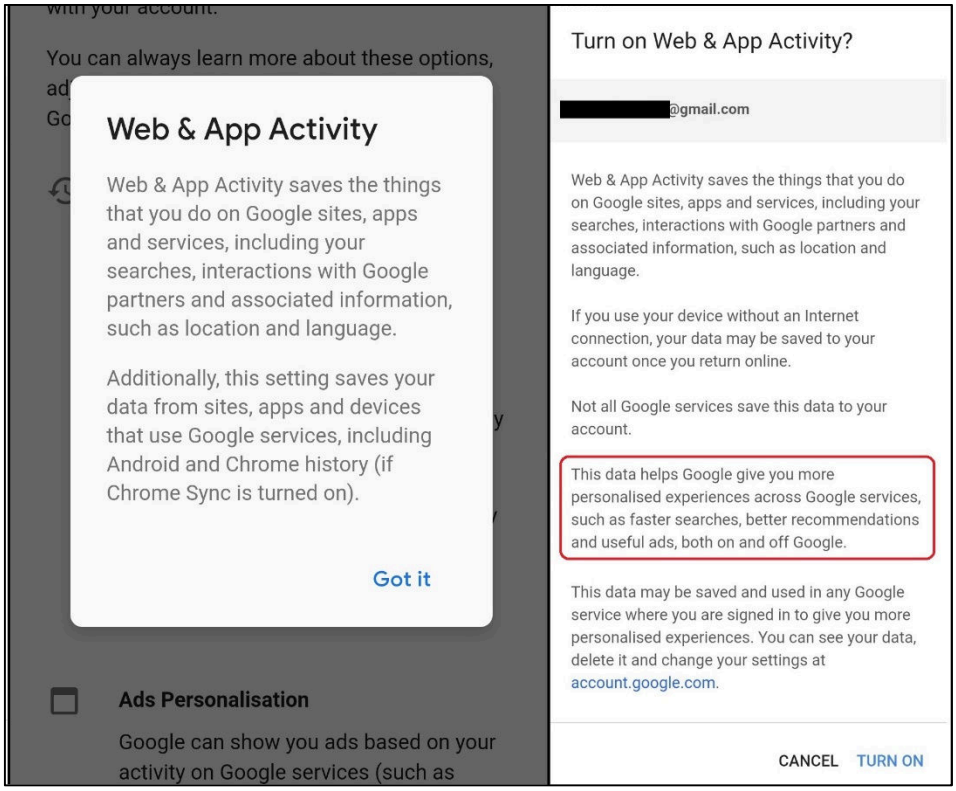
[31] "Google Timeline" https://www.google.com/maps/timeline?pb

[32] "Google privacy policy – How do I know if my Location History is on?" https://policies.google.com/technologies/location-data#is-on

[33] "Google – My Activity" https://myactivity.google.com/myactivity

apps they have used on their Android device. Web & App Activity can also track offline behavior, such as credit card purchases.[34] Web & App Activity is enabled by default when setting up a Google account.

Data from Web & App Activity is also used to personalise advertising. However, information about this data being used for advertising is only shown to the user in certain circumstances. In some contexts, such as when setting up a Google account, the use of this data for advertising is not mentioned, even after clicking "learn more". In a few limited contexts, such as when the setting has been actively turned off, and the user attempts to enable it again, Google informs the user about the advertising purposes.

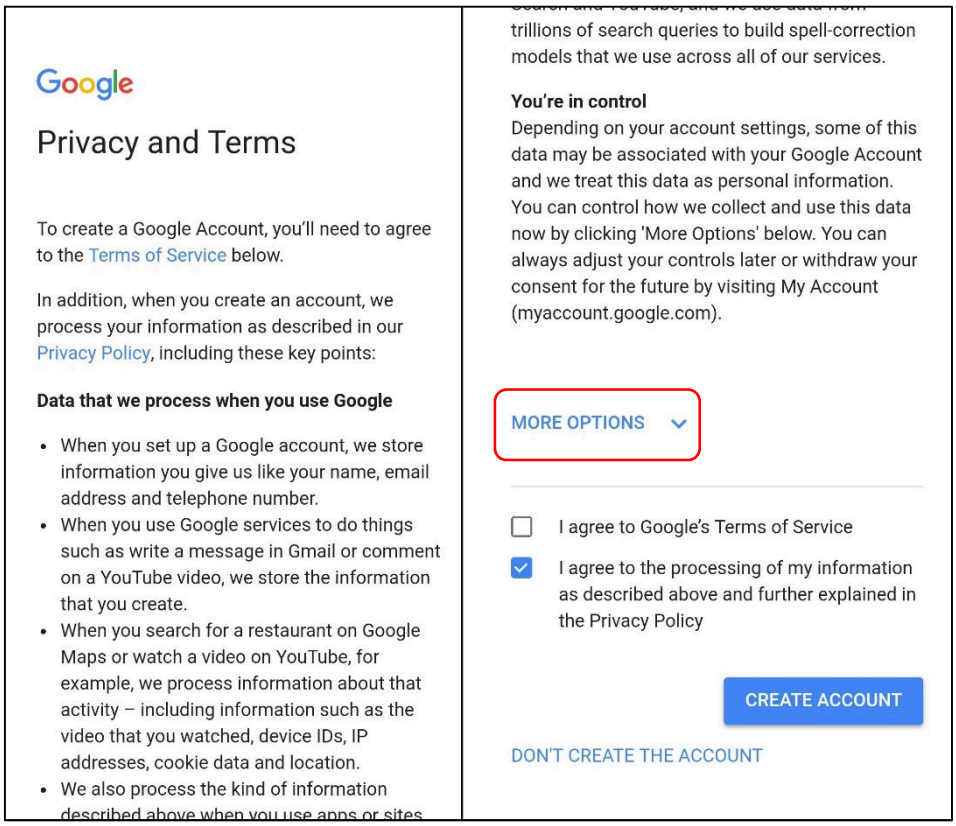


4 Information about Web & App Activity. During the Android setup process (left), and in the Google account (right).

4.3 Setting up a Google Account

When setting up a Google account, users are asked to review a truncated version of Google's privacy policy. In addition to clicking "Create Account", users can click "More options", which reveals a number of settings that can be adjusted.

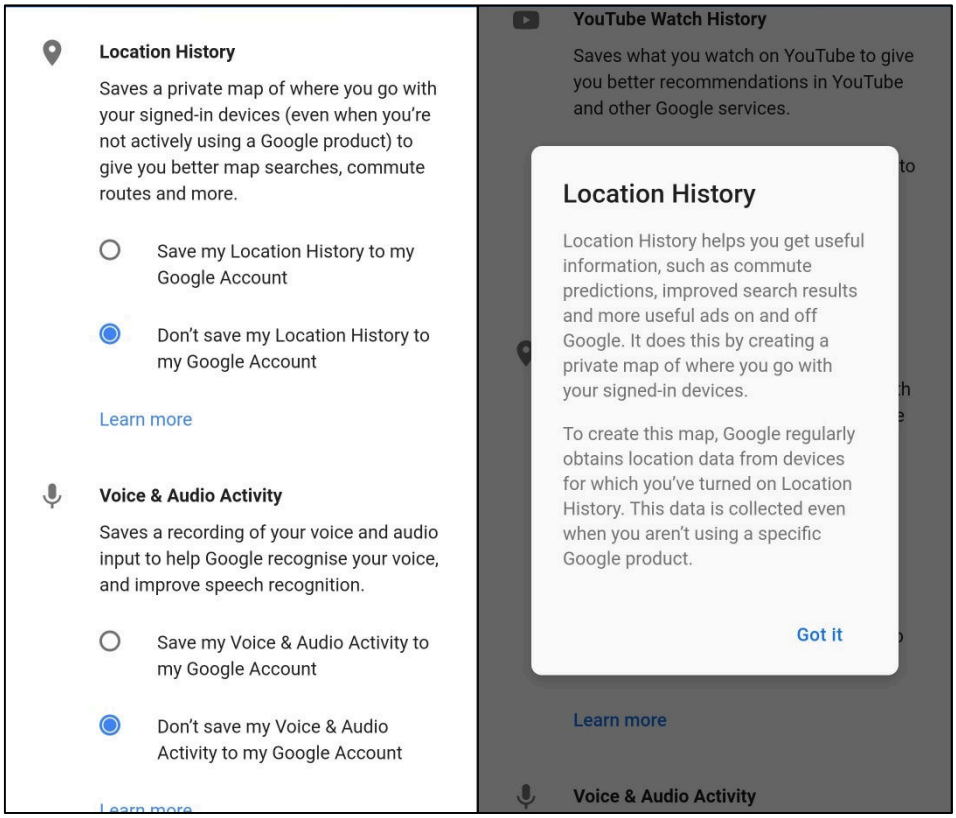
[34] "How to use Google privacy settings"
https://www.consumerreports.org/privacy/how-to-use-google-privacy-settings/



5 Users have to click "More options" to adjust the Google settings.

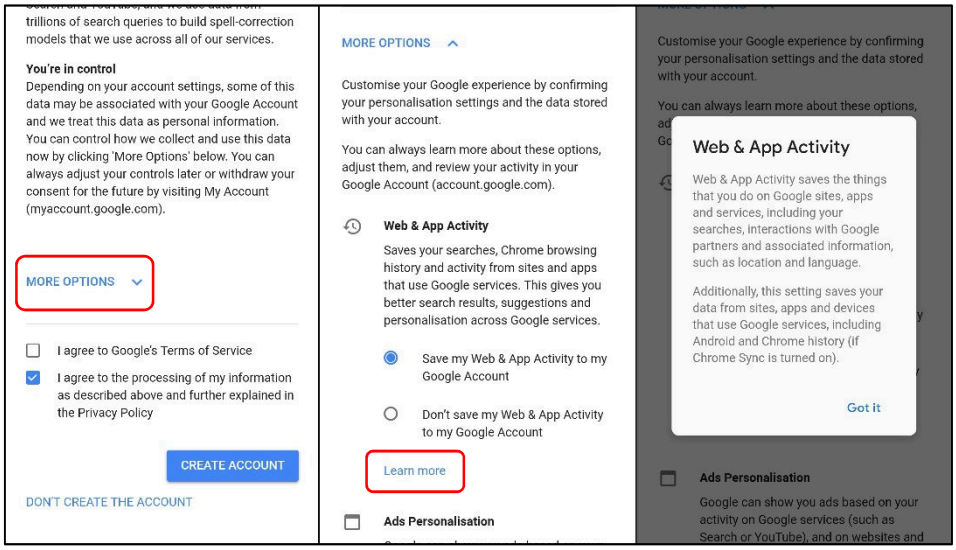
As the screenshot below illustrates, Location History is turned off by default when setting up the account. Note that there is no clear indication that this information is also used for advertising purposes, unless the user clicks “Learn more”. Clicking “Learn more” reveals that the location data collected through Location History is used to serve “more useful ads on and off Google”.[35]

[35] Screenshot of the whole screen and text is included in the appendix.



6 Location History when setting up a Google account.

After clicking "More options", it is also revealed that Web & App Activity is turned on as a default setting. The description beneath the setting says that it provides "better search results, suggestions and personalization". Note that there is no obvious indication that Web & App Activity will record location data, unless the user clicks "Learn more". Neither text mentions advertising.

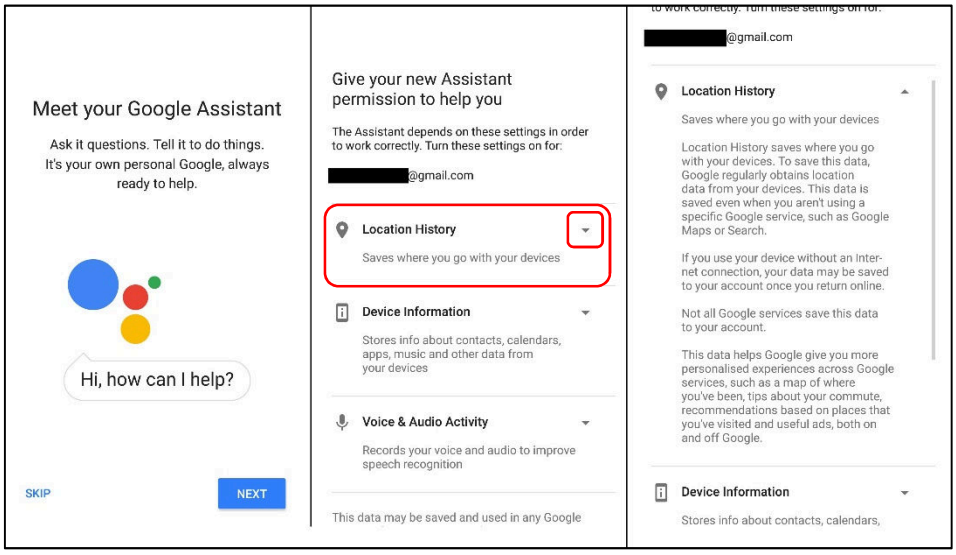


7 Web & App Activity is enabled by default.

4.3.1 Enabling Google Assistant

As part of the process of setting up an Android device, users are asked to enable a service called Google Assistant. Google Assistant is a voice-activated digital assistant, meant to help users perform everyday tasks. The assistant is also an integral part of the Google Home smart speaker system, and several other products made by both Google and third parties. This means that the Google Assistant is likely to become a fixture in the everyday life of many consumers.[36]

As the screenshots below shows, enabling the Google Assistant service in the Android setup process, also entails turning on Location History. On this screen, users are only told that Location History "saves where you go with your devices". If the user clicks the inconspicuous grey arrow to the right of Location History, a more detailed description appears, including the fact that the data is used for advertising purposes.



8 Google Assistant prompt, when setting up an Android device.

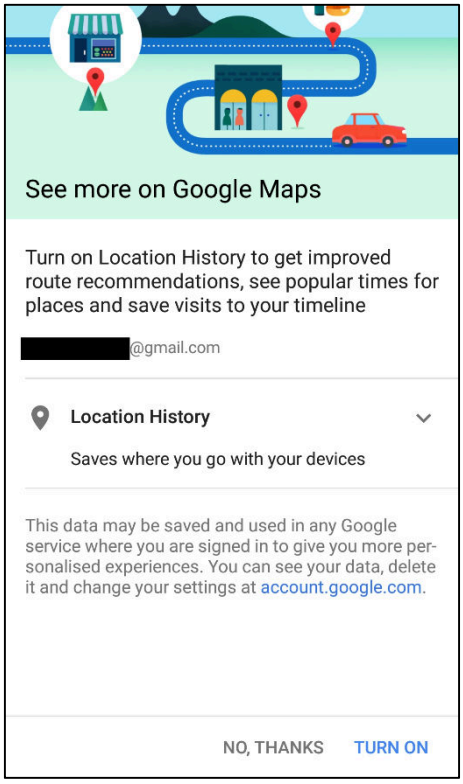
4.3.2 Starting Google apps for the first time

If the user has not enabled Location History when setting up their Android device, they will be asked to enable the setting on several other occasions.[37]

[36] "Google Assistant" https://assistant.google.com/platforms/speakers/

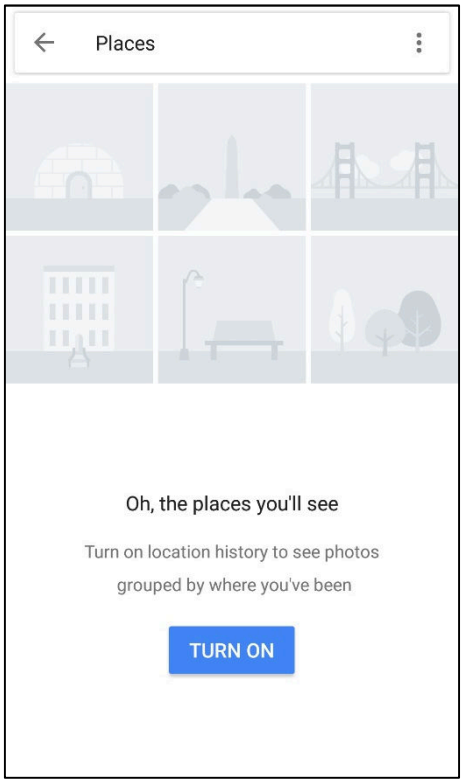
[37] For this test, we only tried starting the preinstalled Google apps after a fresh Android install. We did not observe prompts to enable Location History during the startup of the Google apps YouTube, Chrome, Hangouts, and Drive.

Upon opening the Google Maps app for the first time, users are asked again to activate Location History. The pop-up says that Location History will give users "improved route recommendations, see popular times for places and save visits to your timeline". Unless the user clicks the inconspicuous arrow on the right, they will not be informed that this information is also used for marketing purposes.



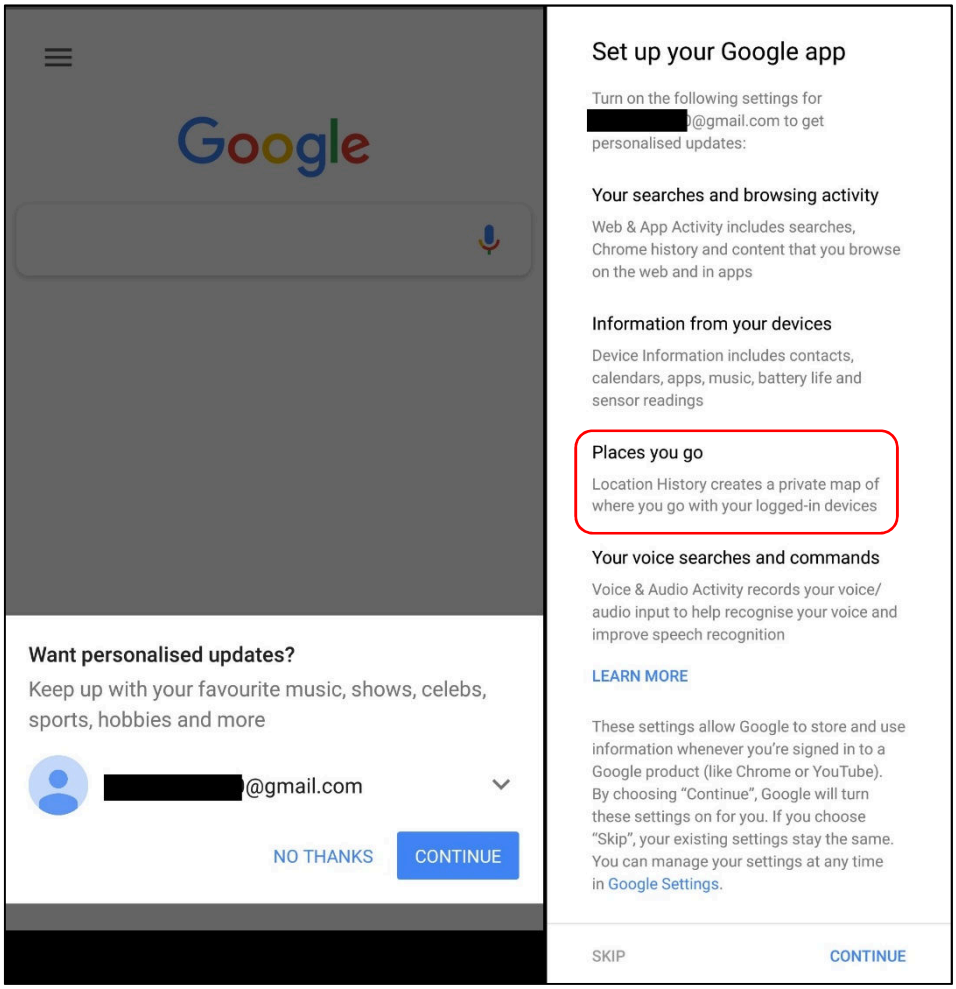
9 Location History prompt when opening Google Maps.

Upon opening the Google Photos app and clicking the "Places" gallery button, users are also asked to turn on Location History. According to Google, enabling Location History lets the user "see photos grouped by where you've been". It does not appear to be possible to enable this particular feature without enabling Location History.



10 Location History prompt when opening "Places" in Google Photos.

Upon opening the Google App for the first time, users are asked once more to enable Location History. As the screenshot below shows, there is no visible information about what enabling Location History actually entails, and there is no obvious button to display more information about Location History before activating the service as a part of “personalised updates”.

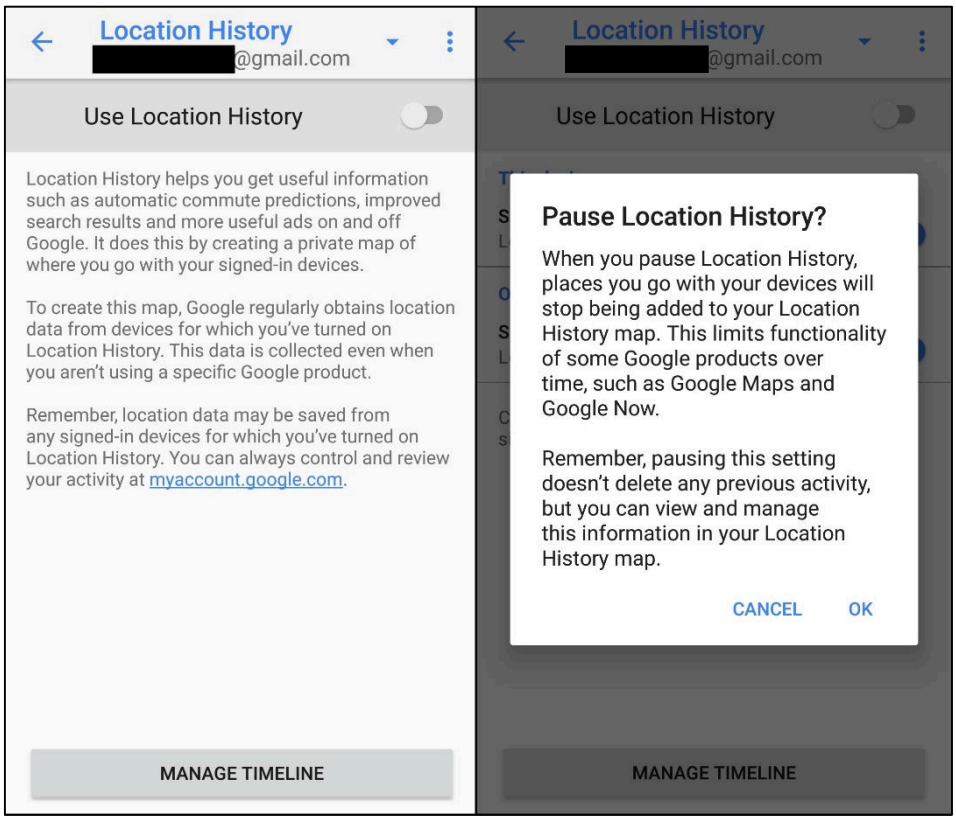


11 Popup when opening Google App for the first time.

4.3.3 Pausing Location History

It is possible to turn Location History on, or to pause it, in the Android location settings menu. As the screenshots below demonstrate, the information given here is somewhat truncated, but informs users that the data collected through Location History is used for ads.

Attempting to pause the service results in a warning that pausing it "limits functionality of some Google products over time". However, there is no comprehensive explanation of all services that are affected, or how their functionality will be limited.



12 Location History in Android settings.

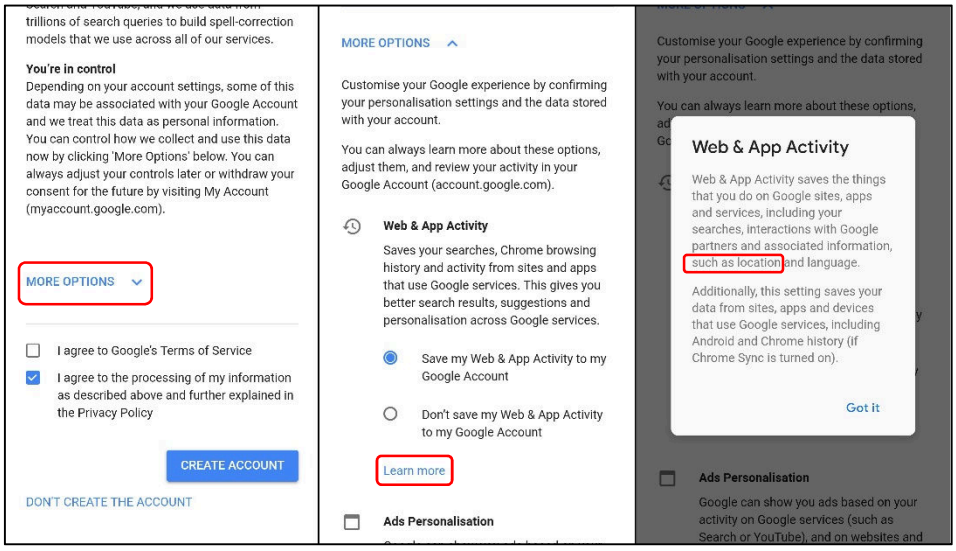
It is also worth noting that there is no real option to *turn off* Location History once it has been enabled; users can only *pause* it after the Google account has been created. This raises questions about whether the user has actually withdrawn his or her consent to the use of past location data for advertising, or if pausing Location History only halts the collection of future data. The process of deleting historical location data is separate from pausing Location History, and Location History data is seemingly retained indefinitely if the user does not actively delete it.[38]

4.4 Location tracking through Web & App Activity

If the user has purposefully avoided enabling Location History, this does not necessarily mean that Google is not collecting the user's location. A report published by the Associated Press in August 2018 showed that Web & App Activity also reports user location data to Google, which is used for

[38] In March 2017, the Danish Consumer Council filed a complaint with the Danish data protection authority against Google. This complaint alleges, amongst other things, that Google retains Location History data indefinitely without a sufficient legal reason to do so. "Forbrugerrådet Tænk anmelder Google til Datatilsynet» https://taenk.dk/om-os/presserum/forbrugerraadet-taenk-anmelder-google-til-datatilsynet

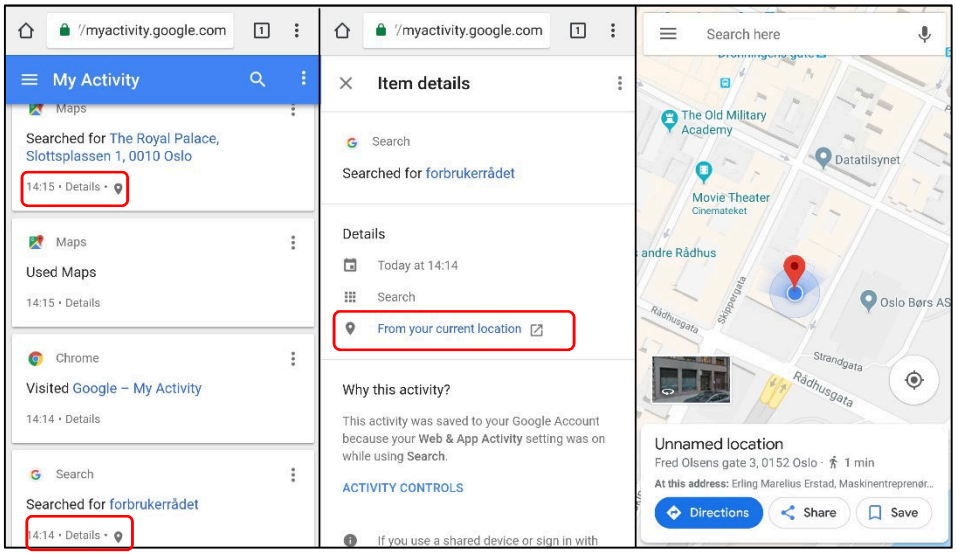
personalisation purposes such as advertising.[39] As mentioned, Web & App Activity is enabled by default when setting up a Google account. Unless the user first clicks “More options”, and then “Learn more”, it is not clear that this setting actually collects location data.



13 Web & App Activity when registering a Google account.

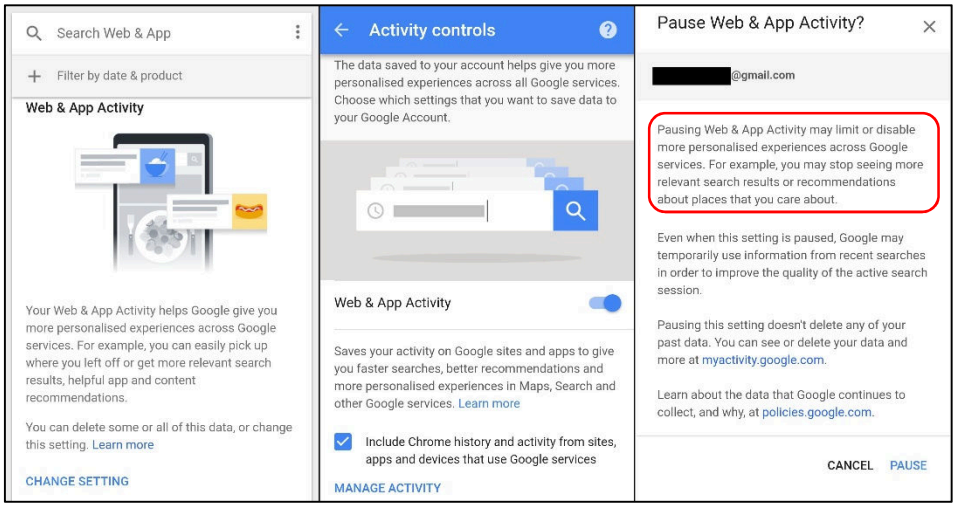
Although most apps do not record the user’s location through Web & App Activity, certain apps and services, such as Google searches and searches made through Google Maps, are logged with location data of where the user was when he or she performed the search. In other words, users who turn Location History off, but leave Web & App Activity on, will still have some of their location data collected by Google. Location data logged through Web & App Activity is not visible on the timeline map that Location History provides, but shows up if the user looks at the My Activity timeline, which is wholly separate from Location History.

[39] “Google tracks your movements, like it or not” https://apnews.com/828aefab64d4411bac257a07c1af0ecb



14 Location data recorded through Web & App Activity

As with Location History, users who attempt to pause App & Web Activity receive a vague warning that this will limit or disable functionality. This non-extensive list includes “you may stop seeing more relevant search results or recommendations that you care about”.



15 Pausing Web & App Activity

4.5 Problematic practices

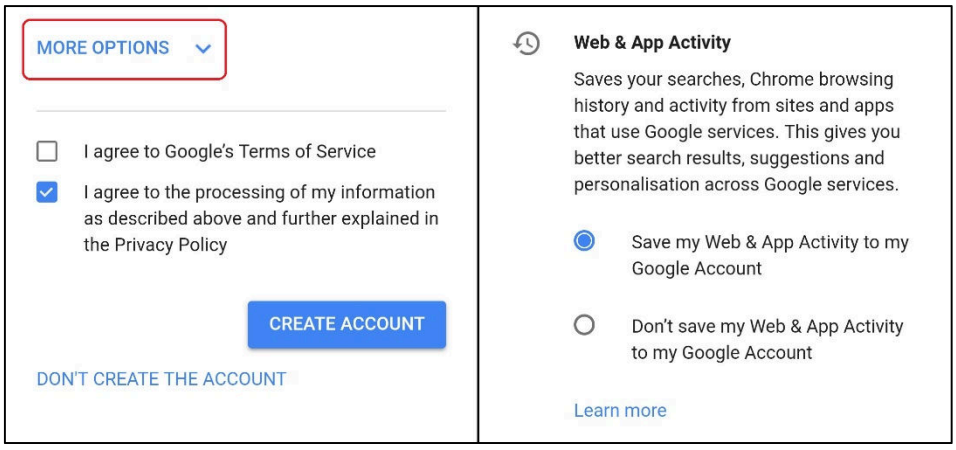
As outlined above, we see a number of problematic ethical and legal issues with the ways that Google have implemented Location History and Web & App Activity into the Google account and the Android operating system, and how they present these settings to the user. In the following, we expand upon the problematic issues, followed by a legal analysis of how the issues are, in our opinion, at odds with the GDPR.

Google give a certain degree of control to the user through its account system. For example, Location History can be deleted through the Location Timeline, and can be exported through Google's "Takeout" tool.[40] However, the data extracted through Takeout seems to be more detailed than what is shown in the Location History timeline.[41]

Users that delve into the dashboard can also get a certain degree of control over what ads they see.[42] Additionally, there is a lot of different information and settings spread throughout the Google dashboard, although some of these can be difficult to find.[43]

4.5.1 Hidden default settings

When setting up a Google account, the actual account settings are hidden behind extra clicks. Users first have to click "More options" to see what the settings are, and whether they are enabled or disabled. Web & App Activity is enabled by default, meaning that users who did not click "More options" will not be aware that this data collection is happening.



16 Default settings hidden behind "More options".

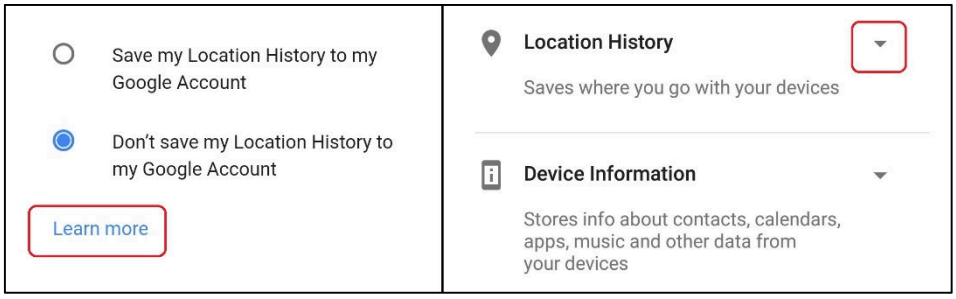
Users are unlikely to diverge from default settings, either because they are in a rush to use a service, or because they trust the service-provider. In any case,

[40] Google Takeout https://takeout.google.com/settings/takeout
[41] This can be seen by using third party tools such as Location History Visualizer https://locationhistoryvisualizer.com/
[42] Google Ads Settings https://adssettings.google.com/
[43] In "Deceived by Design", we documented some of the hurdles of navigating through the Google account dashboard. See pp. 34-39 https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

obscuring the invasive default settings is a dark pattern that dissuades users from making an active choice, and does not provide data protection by default.

4.5.2 Misleading and unbalanced information

Whenever the Location History and Web & App Activity settings are presented to the user, the clearly visible information is limited to a few positive examples of what the setting entails. The information that is visible often also trivializes the extent of tracking that is going on, and how it is used. For example, in all the instances where users are asked to enable Location History, the fact that this data is also used for advertising is hidden behind a grey arrow or a "Learn More"-link.



17 Relevant information hidden behind extra clicks.

Similarly, the fact that Web & App Activity collects location data is also always hidden behind another click, and information about this data being used for advertising is only available in some contexts. Consequently, users are not given sufficient information to make an informed choice. This appears to be cherry picking from the service-provider's side, where certain aspects that may be perceived as negative by the user are glossed over.

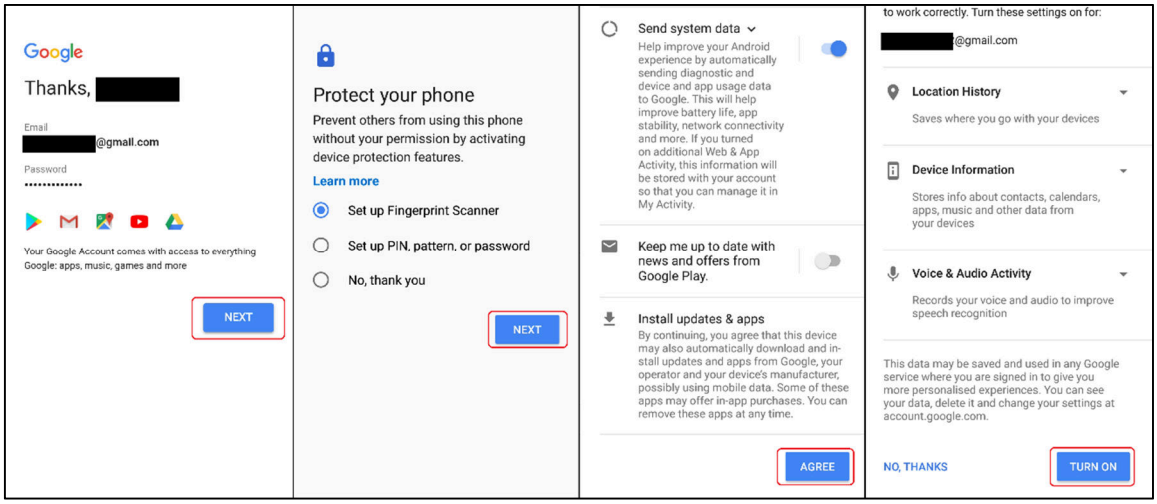
Even if the user clicks "Learn more", the description of both Location History and Web & App Activity still seems to mislead the user about what they are actually agreeing to. For example, Location History is often described as being a "private map", which may give the impression that the information is not used for other purposes such as advertising. Similarly, the name "Web & App Activity" obscures the fact that the setting also collects location data.

4.5.3 Deceptive click-flow

Although Location History technically has to be enabled before it begins collecting data, users following the click-flow when setting up an Android device are likely to unknowingly enable the setting. Google has designed the Android

setup choice-architecture in a way that facilitates enabling Location History as part of the setup process.

As shown below, throughout the setup process, the way to proceed is represented by blue buttons on the bottom right of the screen. However, if the user keeps clicking the blue buttons throughout the process, they will also enable Google Assistant, which means that Location History is also turned on. In other words, users that do not want to share their location with Google have to be very attentive in order to stop location tracking. This is a dark pattern that may end up both irritating and confusing a potentially impatient user into enabling Location History without being aware of it.

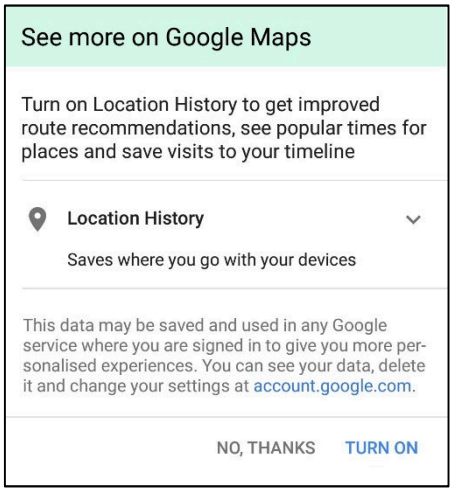


18 Some steps from the Android setup process. Google Assistant prompt on the right. Note that this is a shortened version of the actual process.

4.5.4 Repeated nudging

Users are repeatedly asked to turn on Location History, in many different contexts. On Android devices, users that do not wish to enable Location History have to decline the setting at least four times when using different services that are preinstalled on Android phones;[44] in Google Assistant, Google Maps, Google app, and Google Photos.

[44] Google Maps and Google Photos also ask users to enable Location History on iPhones, but since iOS has different preinstalled services, we regard the nudging as more pressing on Android devices.



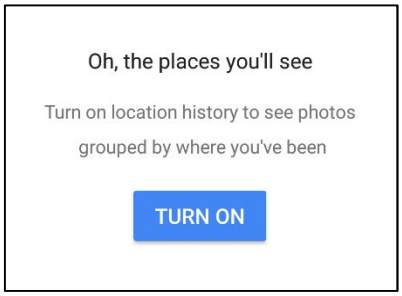
19 Prompt in Google Maps to enable Location History.

Instead of Google taking "no" for an answer, users have to keep making the same choice repeatedly. This increases the chances that users turn on the setting, either by accident, because they are tired of being asked, or because they believe that the services will not work otherwise.

4.5.5 Bundling of services and lack of granular choices

Throughout the Google ecosystem of services, separate services or functionalities are integrated and co-dependent, or simply bundled together. Enabling Location History is required in order to enable other services that users may want to use, such as Google Assistant and Google Photos Places.

Having your photos grouped by location may be a useful and desirable feature for many users. However, in order to enable this feature, users must also enable Location History. There is no granularity to this choice, meaning that users that want their photos grouped by location can only receive this feature by opting in to location tracking for advertising purposes.



20 Prompt in Google Photos to enable Location History.

Similarly, when enabling Google Assistant as part of the Android setup process, users also have to enable Location History. Despite this, the Google Assistant

service appears to function even if the user later disables Location History, although the user is never informed about this.[45]

Conversely, there is no granularity to the actual Location History setting. Either users have to allow Google to collect their location data at all times through Location History, or they must reject the feature in its entirety, blocking off other services that have Location History bundled into them.

In other words, if the user does not allow Google to collect user location data at all times through Location History, Google appears to block off potentially useful features such as Google Assistant and photos sorted by location. This all-or-nothing choice benefits Google at the cost of failing to respect users by for example providing granular choices.

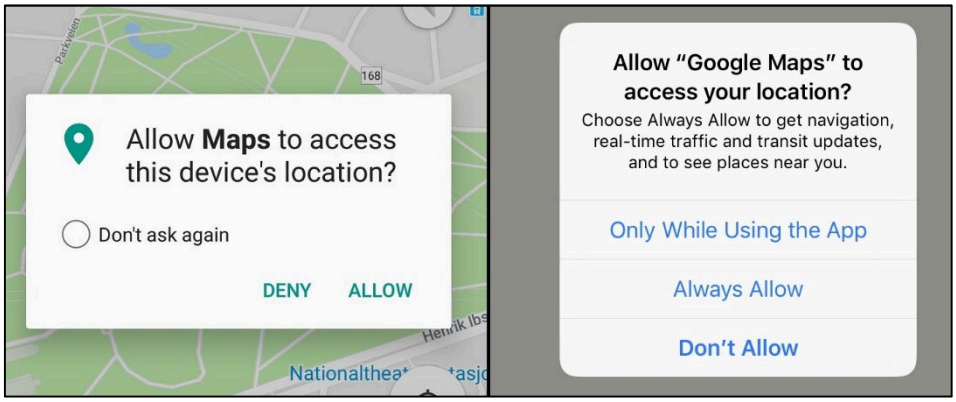
4.5.6 Permissions and always-on settings

When enabled, Location History is always on in the background on Android devices, regardless of whether the user is actively using a service that requires location services. In part, this seems to be because of how the Android operating system works.

Android users that want to use an app that requires location data, have a binary choice; Either they give the app permission to use location services, in which case the app can also record user location when the app is not in use. The alternative is to deny the app permission completely, which means that the app cannot use location services even when in active use.

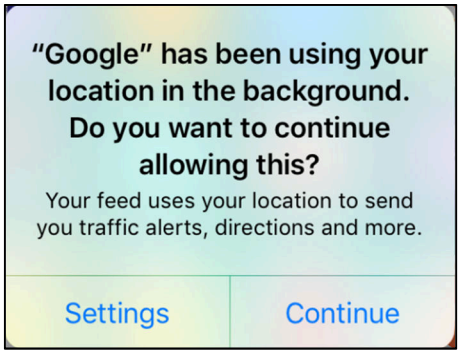
On iPhones, on the other hand, users can choose to give an app permission to use location services only when the app is in use. The latter practice is an example of privacy-preserving technology, while Google's solution is an all-or-nothing choice that limits the users' options.

[45] "If you're using an Android phone, Google may be tracking every move you make" https://qz.com/1183559/if-youre-using-an-android-phone-google-may-be-tracking-every-move-you-make/



21 Device level permissions. Android on the left, iOS on the right.

Additionally, if the user has allowed an app to access location in the background, iOS will periodically remind the user that this is happening. This prevents the user from enabling tracking in one context for a specific reason, then forgetting to turn it off.



22 iOS reminder that the user has given the Google app access to location, even when the app is not in use.

4.5.7 Summary of problematic practices

As users rarely change their settings or break the click-flow when installing software, many are likely not to realize that they turned on Location History,[46] or that Web & App Activity is enabled. Through a variety of dark patterns, Google is getting a blanket permission constantly to collect the exact location of the user, including the latitude (e.g. floor of the building) and mode of transportation, both outside and inside, to serve targeted advertising.

Users that are setting up their Android device, and are eager to get the device up and running, are particularly susceptible to inadvertently turning on Location History, while anyone who want to use Google Assistant when setting up their

[46] In July 2018, Google began sending monthly emails to users with Location History movement. These emails give some aggregated information about the user's monthly travels, but do not mention any other ways that this data is being used.

Android device will end up enabling this pervasive tracking. Furthermore, if the user has kept Location History disabled despite the continued nudging, his or her location will still be shared with Google through Web & App Activity.

In our opinion, the sum of these practices is that users are deceived into enabling privacy adverse features. This deception is unethical, and fails to respect user agency. In the following chapter, the practices will be discussed in the context of European data protection legislation.

5 Legal analysis

In this chapter, we examine whether Google has fulfilled the legal requirements under the GDPR when using location data collected through "Location History" and "Web & App activity" for advertising purposes. For the purposes of this chapter, the terms "data subject" will be used interchangeably with "user", and "data controller" will be used to mean Google.

As demonstrated in chapter 3.5, location data is personal data – information that directly or indirectly can identify a natural person.[47] This means that Google is collecting personal data when it collects and stores information about a person's location and movement through "Location history" and "Web & App activity".

The processing of personal data is only lawful if one out of six general terms is fulfilled.[48] When considering the legal grounds for Google's processing of location data for advertising purposes, we will therefore begin with establishing what legal basis Google is using. In order to establish this, we have used Google's European privacy policy as the main source.[49]

From the privacy policy, it appears that Google is relying both on user "consent" and on "legitimate interests" when processing location data for advertising purposes.[50] It is not clear from the privacy policy which legal grounds applies to what manners of processing. This is in itself problematic, as Google has an obligation to be specific about what legal grounds it is using for particular processing of personal data.[51] Relying on legitimate interest to process data while the processing could have been based on another lawful basis, also constitutes a violation of transparency requirements.[52]

---

[47] GDPR art. 4(1)

[48] GDPR art. 6. See also GDPR recital 40.

[49] "Google privacy policy" https://policies.google.com/privacy#enforcement

[50] On the basis of Google's European privacy policy, this report will not consider other legal grounds than "consent" and "legitimate interest" in art. 6 GDPR for Google's processing of personal data through Location history and Web & App activity

[51] As a result of an investigation done by the EU Data Protection Authorities, Google was already in 2012 urged to clarify which legal basis it uses for processing of personal data. See https://www.cnil.fr/sites/default/files/typo/document/20121016-letter_google-article_29-FINAL.pdf and https://www.cnil.fr/sites/default/files/typo/document/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf

[52] GDPR art. 5(1)(a) see also https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/

To be compliant with GDPR, consent has to be opt in. Because Location History is based on users opting in (off by default), we will assume that this data processing is based on consent.[53] Web & App Activity is turned on by default, and we anticipate that Google cannot rely on consent as a legal basis. The Article 29 Working party clearly state that "pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement" is invalidate consent under the GDPR.[54] Therefore, we assume that processing of location data collected through Web & App Activity is based on legitimate interests.[55]

In the following we analyze whether the way that Google collects consent for Location History is in accordance with the requirements set forth in the GDPR. This is followed by a discussion of the legal grounds for Web & App Activity.

5.1 Consent

Consent is defined in the GDPR as "any freely given, specific, informed and unambiguous indication" by a "statement" or by "clear affirmative action" from the data subject.[56] All of these conditions need to be fulfilled for consent to be considered valid. Below we will look at whether Google's use of Location History data for advertising purposes fulfills these conditions.

In Google's privacy policy, it states:

> "*We ask for your agreement to process your information for specific purposes and you have the right to withdraw your consent at any time. For example, we ask for your consent to provide you with personalized services like ads. We also ask for your consent to collect your voice and audio activity for speech recognition."*

From this, it appears that Google is relying on consent as a legal ground for at least some of its processing of personal data, particularly for serving targeted advertising.

---

[53] GDPR art. 6 (1)(a). See also art. 5(3) of the ePrivacy Directive which requires consent to pull information from a user's device. As the ePrivacy Directive already requires consent for reading information (such as location data) from a user device, it makes most sense if the applicable legal basis under the GDPR is also consent in Location history.

[54] Working Party 29"Guidelines on Consent under Regulation 2016/679" p. 16. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

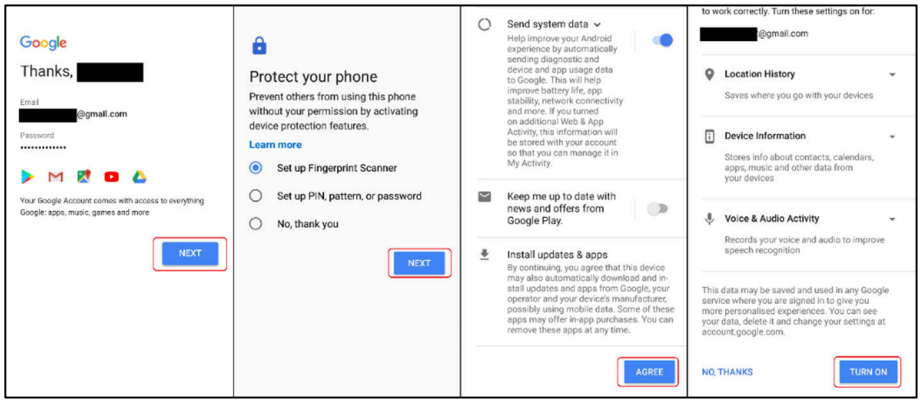
[55] GDPR art. 6(1)(f)

[56] GDPR Art.4(11)

5.1.1 Freely given

Since, as Google argues, users have to opt in to Location History,[57] the data subject should freely have given his or her consent for processing of personal data collected through Location History. This indicates that the data subject has been provided with a real choice about whether he or she accepts Google processing such data, and that this data may be used for advertising purposes.

However, as demonstrated in chapter 4, there are significant differences in how Google collects consent for Location History between iOS-users and Android users. During the Android setup process, users are guided through a process that seems designed to make users consent to Google processing their location data, simply by following the click-flow.



This click-flow makes the user likely to enable Location History as a part of the process, without being made fully aware of what this entails. If the user was not aware what he or she consented to, it will be contestable whether consent has been freely given. Furthermore, if the user has not given consent to Location History during the setup process, Android users are nudged toward enabling the setting at several other occasions. The user may feel pressured into giving his or her consent because of this recurrent nudging.

This is problematic, considering consent should be freely given in order to be valid. "The Article 29 Working Party" have stated that consent is not freely given if there is "any element of compulsion, pressure or inability".[58] Additionally,

[57] "Google privacy policy" https://policies.google.com/technologies/location-data#is-on

[58] "The Article 29 Working Party" was replaced by the European Data Protection Board (EDPB) on the 25th of May 2018. This is a group consisting of EU member state data protection authorities, who provide guidelines on how to interpret EU-regulation on data protection issues. Working Party 29"Guidelines on Consent under Regulation

users are pushed into giving consent to Location History in order to get access to Google Assistant, and to have photos sorted after location. There are also vague warnings about reduced functionality if the user disables Location History. These examples indicate that users who have been nudged into enabling Location History have not "freely given" their consent, and consequently it is not the valid consent required under the GDPR. If this is the case, the processing of this personal data may lack a valid legal basis.

5.1.2 Specific and informed?

In order to be considered valid, consent must be specific and informed. This means that the user must be presented with any information that is necessary to understand what he or she is consenting to, and that it should be clear what the consequences of giving consent could be.

When setting up a Google account, users are told that they can control how Google collects and uses their data. Users are also informed that they can adjust the settings and withdraw their consent. This shows that Google has provided information about rules, safeguards and rights. However, it is questionable whether the way that this information is presented is sufficient, considering users have to click "learn more" to get important information about the purposes of the processing, and the choices they have.

It is also questionable whether Google provides sufficient information about the purposes of the processing of location data. As shown in chapter 4, Google gives some information about processing personal data for advertising purposes, but only if the user clicks "learn more", and even then, this information is vague. Furthermore, phrasing such as "private map" can also mislead the user.

The relevant information regarding what Location History actually entails is hidden behind extra clicks and submenus, and the information about what the data is used for is ambiguous:

> *"Location History helps you get useful information (..) more useful ads on and off Google"*

Even if the consumer finds and reads the information under "Learn more", many users will probably not understand to what extent their location data is processed, that it is stored indefinitely, and how it is used for advertising

2016/679" p. 7 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

purposes. In particular, when using a service such as Google Assistant or photos grouped by location, it may not be obvious for the user that location data is being collected and stored, or for what purposes. This may be at odds with the notion of a "specific and informed" consent.

5.1.3 Unambiguous?

In order for consent to be valid, the user must have given an "unambiguous indication" through a "clear and affirmative action", that he or she consents to Google processing his or her personal data for advertising purposes through Location History.

In this context, it is worth mentioning that if Google was to base the processing of personal data in Web & App Activity on consent, and not legitimate interest (as we anticipate), consent would not be considered "unambiguous" since Web & App Activity is turned on by default. Pre-ticked boxes and "blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data."[59]

Google claims that the user must opt in before it can process location data collected through "Location history". However, since this consent is given after the user has been exposed to dark patterns such as deceptive click-flows and hidden information, it is questionable whether the data subject has given an "unambiguous indication". Furthermore, this raises questions about whether the consent is "obvious". As demonstrated, the user may also have declined to turn on Location History several times, but will continue to be nudged toward turning it on in different contexts.

The user has to perform extra actions, such as clicking "Learn more", to get information about the purpose of the processing of the personal data. The presentation of this information is ambiguous, and consequently may not be in accordance with the requirements for an "unambiguous consent".[60]

[59] Working Party 29"Guidelines on Consent under Regulation 2016/679" p. 16
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
[60] Working Party 29"Guidelines on Consent under Regulation 2016/679" p. 17
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

5.2 Legitimate interests

Processing of personal data may in certain circumstances be based on the data controller's legitimate interests.[61]

According to Google's privacy policy:

> *"We process your information for our legitimate interests and those of third parties while applying appropriate safeguards that protect your privacy. This means that we process your information for things like: […] Providing advertising to make many of our services freely available for users"* [62]

Since data collected through Web & App Activity is used for advertising purposes, and the setting is opt-out, it seems reasonable to assume that Google is relying on legitimate interest as the legal grounds for processing this data.

Under the GDPR, the processing of personal data is lawful if it is "necessary for the purposes of the legitimate interests of the controller".[63] However, if a data controller (in this case Google) is relying on legitimate interests for processing personal data, this must be balanced against the interest or fundamental rights and interests of the data subject. A legitimate interest must also be "lawful", "sufficiently clearly articulated" (transparent) and "represent a real and present interest".[64]

5.2.1 Transparency

As demonstrated in chapter 4, the information provided about the purposes and extent of data collection through Web & App Activity is not particularly clear. The fact that location data is collected as a part of this setting is hidden behind extra clicks, and information stating that this data may be used for advertising is only available under limited circumstances. Additionally, the fact that Web & App Activity is enabled by default is hidden when setting up a Google account.

---

[61] GDPR art. 6(1)(f)

[62] "Google Privacy Policy" https://policies.google.com/privacy#enforcement

[63] GDPR Art. 6(1)(f)

[64] Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" p. 25 and p. 52 www.dataprotection.ro/servlet/ViewDocument?id=1086

Furthermore, in the limited contexts where Google actually provides information about this data being used for advertising, the description of how the data is used is ambiguous:

> *"This data helps Google give you more personalised experiences across Google services, such as faster searches, better recommendations, and useful ads, both off and on Google"*

This phrasing seems like a blanket disclaimer that permits a wide range of purposes for using data collected through Web & App Activity.

Consequently, as the purposes for the collection and use of personal data from Web & App Activity are, in our opinion, unclear, this does not seem to fulfil the requirement for legitimate interest as a legal basis.

5.2.2 Balancing test

In order for legitimate interest to be a valid legal ground for processing personal data, it must be considered whether Google has a legitimate interest that overrides the individual's interests, rights and/or freedoms. This balancing test must be carried out by the data controller.[65]

Several features must be taken into account when performing a balancing test: The nature of the interests of the controller, the possible prejudice suffered by the controller, the nature of the data, the status of the data subject, and the way that data is processed. Additionally, the data controller must take into account the fundamental rights and/ or interests of the data subject that could be impacted.[66]

Privacy and the right to protection of personal data is a fundamental right in the EU.[67] Therefore, there is a high barrier to set aside the individual's rights and interests in privacy matters.

As mentioned, Google states in its privacy policy that it has a legitimate interest to provide "advertising to make many of our services freely available for

---

[65] GDPR art. 6 (1)(f) GDPR and recital 47.

[66] Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" p. 55 www.dataprotection.ro/servlet/ViewDocument?id=1086

[67] Art. 8(1) of the Charter of Fundamental Rights of the European Union, art. 16(1) of the treaty on the Functioning of the European Union (TFEU), art. 1(2) and recital 1 GDPR.

users".[68] However, the extensive tracking performed through features such as Web & App Activity and Location History is very invasive, especially considering that the tracking happens regardless of user interaction, and that the collected data is retained on a seemingly indefinite basis. As a result, Web & App Activity and Location History are arguably privacy adverse. Any legitimate interest to provide advertising should therefore arguably be overridden by the data subject's fundamental right to privacy.

5.2.2.1 Reasonable expectations

In order for a legitimate interest to be valid, it must be considered whether the data subject had "reasonable expectations" at the time and in the context of the collection of personal data, that the personal data could be used for advertising and marketing purposes.[69] This consideration should be based on an objective perspective of what a reasonable person could expect.

It is questionable whether the users had a "reasonable expectation" to believe that Google is tracking their location for marketing purposes in the context of Web & App Activity. In many cases, Google will have been collecting this information since users created a Google account. Today, a number of consumers may be aware of such processing due to the media and consumer organisations contributing to more information and awareness of these practices. Additionally, as shown, Google provides some information to the user.

However, many consumers may not have been aware of this processing when they first created the account. In these cases, the data subject would not have had reasonable expectation for such processing of personal data at the time when Google started collecting the data. Similarly, users who (with or without intent) have enabled Location History, may not have been aware of the extent of tracking and use of the data.

One must also consider whether the context of the collection could give the data subjects reasonable expectations that their location data would be used for advertising purposes. As outlined throughout this report, the extent of the collection of personal data for advertising purposes is under-communicated and hidden in the presentation of both Location History and Web & App activity.

This indicates that many users would not have reasonable expectations about Google processing their personal data for advertising purposes. In addition,

[68] "Google Privacy Policy" https://policies.google.com/privacy#enforcement

[69] GDPR art. 6 (1)(f) and recital 47

since Web & App activity is turned on by default, the data subject would likely not have seen any information about location data being collected, and could therefore probably not have reasonable expectations for such processing, and at such a comprehensive scale.

The Article 29 Working Party recommend that data controllers demonstrate the reasons why they consider their own interest to override the data subject's interests and rights. This should be demonstrated in a clear and user-friendly way. The burden of proof is with the data controller.[70] *In situations where the data subject does not have reasonable expectations of the processing of personal data, this will imply that the data subject's interests and rights will override the controller's interests.*[71] *As the report has shown, Google collects personal data passively in the background and not necessarily while using the app.*[72] *With this in mind, it seems that the lack of a reasonable expectation at the time of collection would tip the balancing act in favour of the interest of the data subject.*

Safeguards

The implementation of certain safeguards can modify the legal grounds for processing personal data using legitimate interests. Such safeguards may include functions such as opting out of the processing of personal data, anonymisations of personal data, and particular transparency measures such as easy to use deletion tools.

Google claims to anonymise data. However, according to recent reports, this "anonymous data" can be easily re-identified as long as the user connects to their Google account.[73] In this case, anonymisation is not actually effective, and works against its purpose as a safeguard.

According to The Article 29 Working Party, "opt-in consent would almost always be required for [...] for tracking and profiling for purposes of direct marketing, behavioural advertisement, location-based advertising or tracking-based digital market research".[74] This implies that Google may lack a valid legal basis to process location data for marketing purposes through Web & App Activity.

---

[70] Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" p. 42 www.dataprotection.ro/servlet/ViewDocument?id=1086

[71] GDPR recital 47

[72] See this report, chapters 3.1 and 3.4.

[73] This is outlined in a 2018 report by researchers at the Vanderbilt University. "Google Data Collection" https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf

[74] Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" p. 47 www.dataprotection.ro/servlet/ViewDocument?id=1086

***

As we have seen, users are able to opt out of Web & App Activity by pausing the setting. However, it is unlikely that many users would ever opt out of Web & App activity, since they would likely not know that the setting is turned on by default. Furthermore, regular users will be unaware that location data is collected, that this data is used for advertising, or even that Web & App Activity exists in the first place.

In our opinion, because of the high barrier to protect the individual's right and interest in privacy matters, Google's interests does not override the data subject's interests and rights in this case.

5.3 Summary of legal analysis

As demonstrated throughout this chapter, the ways that Google has designed its Location History and Web & App Activity settings are problematic in light of European data protection requirements. In this report we have questioned the legal basis Google has for collecting and processing this location data.

It is questionable whether users have given free, specific, informed, and unambiguous consent to the collection and use of location data through Location History. It can also be discussed whether the user can withdraw his or her consent, since there is no real option to turn off Location History, only to pause it.

Since Web & App Activity is turned on by default, the collection and use of personal data through this setting cannot be based on consent. Google claims to have a legitimate interest in serving ads based on personal data, but the fact that location data is collected, and how it is used, is not clearly expressed to the user. This calls into question whether Google's legitimate interest in serving advertising as part of its business model, overrides the data subject's fundamental right to privacy. As we have argued above, in light of how Web & App Activity is presented to users, the interests of the data subject should take precedence in this case.

6 Appendix

Setting up a Google account.

The screenshots show what users are presented with when setting up an Android device. In order to see the different options, and to turn these on or off, users have to scroll through the truncated privacy policy, and click “More options”.