

## Oracle Corporation Submission to the Digital Platforms Inquiry

Thank you very much for providing this opportunity to make a submission to the Australian Competition and Consumer Commission (ACCC) in relation to the Preliminary Report from the ACCC's Digital Platforms Inquiry.

### A. Preliminary comments

1. The ACCC is to be commended for issuing a thorough Preliminary Report, with its preliminary recommendations well supported by compelling evidence. The Preliminary Report shines a light on some important issues, not only for Australia, but globally.
2. In providing this submission to the ACCC, Oracle Corporation (**Oracle**) wishes to focus primarily on the activities of one digital platform, Google, and the way that Google's actions in a number of different areas have had, and continue to have, a detrimental impact on Australian consumers and small businesses. This submission will focus upon how Google exploits consumers and small businesses and in doing so forecloses competition in advertising markets. This, as is further explored in the Preliminary Report, has had follow-on negative impacts in the media sector in Australia.
3. Oracle believes it is important that, through the investigations by agencies such as the ACCC, Australian consumers are able to understand the extent of the personal information that is gathered by Google on them, how it is gathered and how it is used (including how Google combines information to infer other personal information that the consumer did not intend to provide). Without this understanding it is difficult for consumers to determine the value of their personal information or make informed and real choices. Such investigations and independent analysis, as has been undertaken by the ACCC, also demonstrate how Google, by acting in an unconstrained manner, creates barriers to competition that need to be addressed in a timely manner to the benefit of consumers and the competitive process.
4. The preliminary recommendations that the ACCC has made to address the behaviour of Google, as well as the investigations that we understand the ACCC is undertaking which are referred to in the Preliminary Report and which Oracle has supported in this submission, will in our view assist in addressing the behaviour of Google. The recommendations and the guidance provided by the outcome of the investigations will also assist in ensuring that, in future, no other company will be able to abuse substantial market power obtained from its dominant position, in the manner that Google has been able to in the relevant online markets. This is important as Google's anticompetitive behaviour has resulted in such negative impacts for Australian consumers and small business as well as for the competitive process.
5. In our view the key regulatory solutions are simple:
  - (a) Action should be taken under existing Australian law, including the Australian Consumer Law and the Privacy Act 1988 (Cth) (**Privacy Act**), where Google's activities are shown to breach that existing law. Those existing regimes provide both the ACCC and the Office of the Australian Information Commissioner (**OAIC**) with tools to take action against Google immediately in respect of issues identified in the Preliminary Report, without the need to wait for the ACCC's report to be finalised or for the Australian Government to respond to that report.
  - (b) The Privacy Act should be amended to reflect the changing landscape which faces consumers, and the ongoing challenges consumers have in protecting their personal information. A particularly important change would be to require "voluntary" consent not only to the provision of personal information but also to the combination of that information. This would require that a consumer has the right to use digital platform services that are funded by advertising provided the consumer agrees to receive

advertising and *even if* the consumer does not agree to receive targeted advertising or to the associated collection and combination of his or her personal information. This voluntary consent right should be linked with obligations for platforms to provide clearer and simpler disclosure and a right of erasure.

**B. Preliminary recommendations that are supported by Oracle**

1. Oracle wishes in this submission to focus upon certain of the ACCC preliminary recommendations due to its technology focus. Oracle makes no comment on the other recommendations contained in the ACCC Preliminary Report. Oracle is particularly supportive of the following preliminary recommendations included in the Preliminary Report:
  - (a) Preliminary recommendation 1: Amendments to Australia's merger law.
  - (b) Preliminary recommendation 2: Requiring prior notice of acquisitions to be provided to the ACCC.
  - (c) Preliminary recommendation 3: Allowing choice for internet browsers and options for search engines.
  - (d) Preliminary recommendation 8: Amendments to Australia's Privacy Act.
  - (e) Preliminary recommendation 9: Requiring the establishment of a Code of Practice for digital platforms, to be developed under the existing Part IIIB of the Privacy Act.
2. We have commented on certain of these preliminary recommendations below.

***Preliminary recommendations 1 and 2: Amendments to Australia's merger law and prior notice***

3. In support of preliminary recommendations 1 and 2, in section 2.3.5 of the Preliminary Report the ACCC has referred to the US\$23 billion that Google is reported to have spent over the decade from 2004 in acquiring companies. These acquisitions have enabled it to entrench its position in search and search advertising. Specific examples that are discussed in detail in that section of the Preliminary Report include Google's acquisitions of YouTube and DoubleClick.
4. Other examples that it is useful to consider in detail are Google's acquisitions of Urchin and AdMob. Both of these acquisitions demonstrate how critical foreclosing competition and acquiring data are in Google's acquisition strategy.
5. Google acquired Urchin, a web analytics firm that (amongst other services) provided programs to companies to allow them to collect and analyse data including traffic on their own sites, in 2005. One of the reasons Google acquired Urchin was to ensure that it could enter and quickly take over third party display advertising markets. At the time, Google did not have its own analytics program and therefore the acquisition of Urchin filled that gap. Google began to develop Google Analytics shortly after it acquired Urchin and at the time stated that it would continue to operate Urchin in parallel. However, Google ultimately did combine the two into a super analytics platform and stopped offering Urchin as a separate product – meaning the acquisition had the effect of “killing off” a potentially vibrant competitor.
6. The Urchin acquisition had another outcome. At the time of the acquisition, Urchin's software could be installed on a private server, allowing the user to retain control and access over its raw data. By ceasing to offer that software product, Google ensured that this tool ceased to be available.
7. The acquisition had a broader data impact as well. Google integrated Urchin's consumer and ad data with its own data. To ensure that it maximised the data advantage obtained from the acquisition, Google significantly broadened the scope of the information it was allowed to combine through changes to its privacy policy introduced on 14 October 2005. These amendments to its policy granted Google the right to "*combine the information you submit*

*under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services", including the "display of customized content and advertising"<sup>1</sup> (even though, "for certain services", Google granted its users "the opportunity to opt out of combining such information"<sup>2</sup>). Therefore, only months after its acquisition of Urchin, Google without prior notice or consultation, permitted itself for the first time to combine information submitted by a user under his or her account with third-party cookies for, among other purposes, advertising.*

8. Google's AdMob acquisition in 2009 is also noteworthy as this eliminated Google's primary competitor for targeted mobile app-based advertising (noting AdMob competed with Google's AdSense at the time) and provided Google with access to a significant amount of consumer data for the most popular mobile apps in the Google Play Store and also the iTunes App Store.
9. The AdMob acquisition positioned Google to capture an enormous share of in-app advertising revenue as AdMob is used by 83% of Android apps and 78% of iOS apps that use at least one advertising platform<sup>3</sup>. AdMob continues to grow, as over 1.1 million Android apps and a similar number of Apple iOS apps include Google ad software<sup>4</sup>. The AdMob acquisition strengthened Google's data position particularly as it provided Google with data about iPhone users, which it would not otherwise have been able to access. As marketing experts opined at the time, *"the biggest reason Google bought AdMob: the data"*<sup>5</sup>.
10. The effect of both of these acquisitions in the digital platforms markets, that is, for online search engine, social media and digital content aggregator services, and in associated online advertising markets, strongly supports a conclusion that antitrust regulators should be able, in any merger analysis in those markets, to take into consideration not only the impact that the acquisition of a potential competitor will have on competition in the relevant market, but also the impact that the acquisition of data will have on competition.
11. We are also supportive of preliminary recommendation 2 for the reasons highlighted in section 2.8.2 of the Preliminary Report. It is difficult to review acquisitions of nascent competitors and predict the likely future in the absence of a proposed acquisition in the digital platforms markets and associated online advertising markets, particularly given that these markets themselves are in a state of technological evolution. This is analysis that the ACCC (and other antitrust regulators globally) should undertake very carefully in respect of acquisitions in such markets; each such review must be undertaken with intellectual vigour and rigorous testing. If entities falling within an appropriate definition of "large digital platforms" provide undertakings, or are otherwise compelled, to provide sufficient notice of proposed acquisitions, this will allow the time needed to ensure that the ACCC is able to properly undertake such an exercise.

#### ***Preliminary recommendation 8: Amendments to the Privacy Act***

12. The fact that the Preliminary Report has considered privacy related issues indicates that, whilst antitrust, consumer protection and privacy issues are distinct, each of these separate areas may need to be considered in assessing the overall impact (both positive and negative) of digital platforms on Australian markets, consumer welfare and the competitive process. In this regard, we agree with the sentiments expressed by Rod Sims' in a recent speech<sup>6</sup> that it is essential consumers are able to make informed and voluntary decisions about how much data is collected

---

<sup>1</sup> Google Privacy Policy, 14 October 2005, emphasis added.

<sup>2</sup> Google Privacy Policy, 14 October 2005.

<sup>3</sup> <http://www.businessofapps.com/majority-of-apps-are-now-using-one-or-more-sdks-for-in-app-advertising/>

<sup>4</sup> <https://www.cnn.com/2018/02/15/googles-app-network-quietly-becomes-huge-growth-engine.html>

<sup>5</sup> Ian Schafer, *Why Google's Acquisition of AdMob Isn't Just About Advertising*, FORBES (10 May 2009), <http://bit.ly/2L8YLOD>.

<sup>6</sup> <https://www.accc.gov.au/speech/insights-and-impacts-of-the-accc-digital-platforms-inquiry>

about them from such digital platforms and how this data is used. In the absence of this, antitrust issues may arise. Therefore by definition privacy issues need to be considered in the context of digital platforms, as do issues of consumer protection more generally, though these should not be confused with the separate antitrust issues which also arise.

13. While we support in principle the proposed amendments to the Privacy Act in preliminary recommendation 8, we have the following further comments:

(a) *Strengthening notification requirements*

The ACCC has recommended that notification requirements are strengthened, including by amending Australian Privacy Principle (**APP**) 5 to require that consumers should be notified of the details of the entity collecting the data, the types of data that is collected and for what purpose and whether the data will be disclosed to third parties (and, if so, for what purpose).

There is an additional piece of information that should be provided to consumers under an improved APP 5. This is information on what other data the collected data will be *combined* with and what personal information is able to be inferred about the consumer as a result of any such combination of data.

Looking, for example, at Google's privacy policy, although many readers of that policy may not realise this, Google is entitled under that policy to combine data that it obtains from many different sources, being data collected through the use by a consumer of any one of Google's "services". Services in this context is very broadly defined in Google's privacy policy to include Google apps, sites, and devices (such as Google search, YouTube and Google Home), platforms like the Chrome browser and the Android operating system and products that are integrated into third-party apps and sites, like ads and embedded Google Maps. Google's "services" therefore also include tools such as Google Analytics.

This means Google may collect and combine data from a consumer's:

- (i) input into Google's services such as the consumer's use of Google Maps (both the search queries that consumers make and the tracking of consumers that occurs through use of Google Maps), Google search and YouTube;
- (ii) browsing activities from both desktop and mobile devices, whether through browsers or apps; and
- (iii) Android device (if the consumer has one, and noting that the Preliminary Report acknowledges it is estimated that approximately 40% of mobile devices in Australia use the Android operating system), including location data – everywhere the consumer has been, how they got there and what they are doing when they are there, and regardless of whether the user is aware of and has positively consented to this information being collected or not.

The collection of some of this data, if looked at in isolation, might be considered innocuous. However, the *combination* of all of these types of data allows Google to build highly specific super profiles of an individual consumer's demographic details, behaviours and interests which is then used to sell advertising. Given that Google's services are used by such a significant number of consumers, this means Google collects such information about a significant number of Australians. This data is collected even where a consumer may not realise that he or she is using a Google service at all, such as where a consumer without a Google Account (and not using an Android device) accesses a website that uses Google Analytics. Google's business model is dependent upon collecting and combining significant amounts of data to obtain a complete picture of as many consumers as possible, and then and leveraging this highly specific personal information to advertisers.

To take a simple example, Google tells its true customers (advertisers)<sup>7</sup>:

*With demographic targeting in Google Ads, you can reach a specific set of potential customers who are likely to be within a particular age range, gender, parental status, or household income.*

...

*When people are signed in from their Google Account, we may use demographics derived from their settings or activity on Google properties, depending on their account status. Consumers can edit their demographic information by visiting Ads Settings. In addition, some sites might provide us with demographic information that people share on certain websites, such as social networking sites.*

*For people who aren't signed in to their Google Account, we sometimes estimate their demographic information based on their activity from Google properties or the Display Network. For example, when people browse YouTube or sites on the Display Network, Google may store an identifier in their web browser, using a "cookie". That browser may be associated with certain demographic categories, based on sites that were visited.*

Google could only infer demographic information with a sufficient degree of specificity to allow it to sell such demographically targeted advertising if it collected, and was able to combine, vast quantities of data about individuals (which it is able to link directly to an individual's device or devices). It is the ability to combine the vast quantities of data that Google holds about individuals quickly and efficiently that allows Google to create "super-profiles", inferring personal information that consumers may simply not have intended to provide to Google. The above quote from Google's website acknowledges not only that that Google is able to create super profiles, but that it does do this, irrespective of whether a person has a Google Account.

In this submission, including the attachments, we have used the term "super profile" to refer to all of the data Google collects on an individual, from whatever source. The term "shadow profile" on the other hand refers to the portion of the super profile data that Google maintains in relation to a consumer that the consumer is unable to access.

As is made clear in the paper entitled "Google's Shadow Profile: A Dossier of Consumers Online and Real World Life", which is at Attachment A of this submission, not only is the information that is currently provided to consumers confusing, but only a small amount of the data Google collects is made available to Google Account holders, even though Google claims to provide an exhaustive list of all the data collected about an account holder to that person. In reality, Google collects and stores significantly more data about each consumer, regardless of their account status, and ties this data to unique identifiers which make it possible to link the information back to an individual.

The super profiles that Google is able to create are available for Google to access at any moment across various products and services and are continuously updated as consumers navigate the internet and the real world. Consumers should be clearly and unambiguously told that this is how Google will use a consumer's personal information when that consumer provides *any* of his or her data to Google through the use of one of Google's ubiquitous "services".

---

<sup>7</sup> <https://support.google.com/google-ads/answer/2580383?co=ADWORDS.IsAWNCustomer%3Dfalse&hl=en&oco=0>

(b) *Strengthen consent requirements and power to the consumer*

*Location data*

The preliminary recommendation from the ACCC is that, where the Privacy Act already requires consent to be given before personal information is able to be collected, this consent is express opt-in consent. This is supported but our view is that the Privacy Act should also be amended to require express opt-in consent where *location data* is collected from any mobile device.

As the US Supreme Court recently noted in the decision of *Carpenter v United States* No. 16-402, 585 U.S. (2018), location data “provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations’”<sup>8</sup>. To avoid all arguments as to whether location data is personal information (though in our view it is both personal information and sensitive information for the purposes of the Privacy Act, which is a point we return later in this submission) and given the intimate details that are able to be inferred about a consumer from location data, its collection should require express consent.

*What is informed consent?*

In section 5.7.1 of the Preliminary Report it is noted that the amendments in preliminary recommendation 8 are proposed to allow consumers greater control over the collection of their personal information. Although the proposals – including the proposal for express opt-in consent – would, if implemented, reduce information asymmetries between consumers and digital platforms such as Google, there is a question of whether the changes would truly increase the level of control for consumers.

This is the case as none of the recommendations go so far as to require that particular digital platform services must be provided in circumstances where a consumer has not consented to the digital platform’s personal information collection policies. In other words, although measures that increase transparency and require positive opt-in by a consumer to provide consent to the collection of personal information would be significant improvements to the current regulatory framework, if a consumer is still effectively compelled to agree to allow personal information to be collected about him or her in order to use particular services such as Google search or to ensure that his or her Android device operates, then the position for the consumer is hardly improved.

***It is for this reason that we are supportive of the proposal raised as an area for further consideration in the Preliminary Report that regulation should be implemented prohibiting digital platforms from collecting, using or disclosing personal information of Australians for targeting advertising unless the relevant consumer has provided opt-in consent and, where the consumer does not opt in, the digital platform must nonetheless provide access to the relevant advertising funded service if the consumer had agreed to accept non-targeted ads.***

In this context, we recommend that the ACCC gives careful consideration to the recent well publicised Bundeskartellamt Facebook decision. The Bundeskartellamt decision recognises the inherent problems arising from allowing dominant digital platforms to *combine* data from different sources. The Bundeskartellamt decision, which is being appealed by Facebook, will require Facebook to obtain a consumer’s “voluntary consent” to Facebook’s practice of *combining* data generated from the use of services owned by Facebook (such as WhatsApp and Instagram) with data from third party websites and apps that use some form of Facebook services such as the Facebook “Like” button or analytical services such as

---

<sup>8</sup> At page 12.

“Facebook Analytics” and then associating that combined data with a consumer’s Facebook account and using that data for a broad range of uses.

The Bundeskartellamt has said that “voluntary” means that use of Facebook’s services must not be subject to a consumer providing such consent (though Facebook may condition use of the Facebook website or app itself on a consumer allowing direct data collection by Facebook from that website or app). In this sense, the Bundeskartellamt recognises that it is the combination of data that leads to a loss of control by a consumer of his or her personal information because by combining such data from a number of different sources Facebook has been able to build a unique database on each individual Facebook user. The same analysis applies to Google. It is Google’s ability to collect a vast amount of data regarding a consumer, both from Google’s own direct services such as Google Search and YouTube and from websites and apps that “partner” with Google (such as websites that use DoubleClick advertising and Google Analytics cookies), which it then combines to create super profiles – in ways that a consumer could not possibly envisage when he or she consented to Google’s privacy policy – allowing Google to sell highly targeted advertising to advertisers. Therefore an equivalent remedy to that proposed by the Bundeskartellamt for Facebook would be equally appropriate in the case of Google.

(c) *Right to erasure*

It has been recommended that consumers have the right to require erasure of their personal information when they have withdrawn consent and the personal information is no longer necessary to provide the consumer with a service.

It should be very clear what is captured by this right of erasure. It should not simply be “personal information” in isolation, for example, a person’s name, address and telephone number, but should also include information that, when *combined* with other information that is (or is able to be) collected by the holder of that information, may be used to infer personal information. That this type of information may be personal information is made very clear not only from the express definitions included in the Privacy Act, but also the APP Guidelines issued by the OAIC<sup>9</sup>. The APP Guidelines expressly state that collection of personal information may take place where a regulated entity generates personal information from the data it holds. This recognises the contemporary reality of how data is collected and used not only by digital platforms such as Google but by other businesses that collect data regarding consumers, both on- and off- line. In the case of data collected by Google, the right of erasure should extend to all of the data that it has obtained about a consumer from that consumer’s use of any of Google’s ubiquitous services.

Clarification is required in the following areas:

- (i) How would an assessment be made of what personal information was “necessary” to provide a consumer with a service? Google’s privacy policy includes within its definition of Google’s services “(p)roducts that are integrated into third-party apps and sites, like ads and embedded Google Maps” as well as “(p)latforms like the Chrome browser and Android operating system”. Could it be argued that the collection of personal information from consumers is ever “necessary” to provide those services? If yes, then it would be very difficult (or impossible in the case of a consumer with an Android device) to ever exercise this right to require erasure of personal information. Consequently, “necessary” should be very narrowly defined.

---

<sup>9</sup> [https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP\\_guidelines\\_complete\\_version\\_2\\_March\\_2018.pdf](https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_2_March_2018.pdf)

- (ii) Appropriate means must be provided for *all* consumers to be able to require the deletion of the personal information that is held about that consumer. Google collects personal information about consumers whether a consumer has a Google Account or not. For example, as explained in our separate paper at Attachment B “Google Stealthily Enables ‘Super-Profiles’”, the tracking and collection of personal information about a consumer will occur if a consumer visits a site that uses Google Analytics (such as the ACCC’s website or the OAIC’s website). Google’s privacy policy allows it to combine the data it obtains from use of any such site with any other data it has in relation to the same device, which will allow it to develop a super profile for, and infer significant personal information about, the holder of that device. In the case of Google, where a person does not have a Google Account, not only is there currently no way for a person to determine what personal information Google holds about him or her, there is no way for that consumer to request that all such personal information that has been collected is deleted. (As an aside, it is of course a breach of the existing APPs that a consumer without a Google Account is unable to request access the personal information that is held about him or her by Google, given APP 12 provides that, subject to certain exceptions, a regulated entity, must provide to an individual access to the personal information of that individual if he or she requests it.)

**C. Investigations under the Competition and Consumer Act 2010 (Cth) (CCA)**

1. In Chapter 5 of the Preliminary Report, it is noted that the ACCC is investigating the conduct of certain digital platforms under the CCA including (amongst other matters):
  - (a) An investigation of whether a particular digital platform’s representations to users regarding the collection of particular types of data may have breached the Australian Consumer Law. This is referred to below as **Investigation A**.
  - (b) Investigating potential breaches of the Australian Consumer Law relating to changes to a digital platform’s privacy policy that may enable the digital platform to combine different sets of user data. This is referred to below as **Investigation B**.
  - (c) Investigating whether digital platforms’ terms of use and privacy policies may contain unfair contract terms under the Australian Consumer Law. This is referred to below as **Investigation C**.
2. Oracle wishes to provide the further information set out below in relation to each of these investigations, which may assist the ACCC in these matters.

*Investigation A*

3. Although not stated in the Preliminary Report, we believe that Investigation A may relate to the collection of location data by Google. If this is not the subject of this investigation, our strong view is that this should be investigated.
4. At Box 5.9 of the Preliminary Report, reference is made to the fact that Google’s website stated, until at least August 2018, “You can turn off Location History at any time. With Location History turned off, the places you go are no longer stored.”
5. Section 18(1) of the Australian Consumer Law provides that “(a) person must not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive”. Whether a statement is misleading or deceptive is a question of fact to be determined in all of the circumstances in question. For the reasons outlined in the Associated Press article referred to at Box 5.9 of the Preliminary Report there is in our view strong support for an argument that the statement referred to in the previous paragraph is misleading and deceptive for the purposes of section 18(1) of the Australian Consumer Law.



6. However, there is also the question of whether the statements that are *currently* included on Google’s website (including but not limited to its privacy policy) in relation to the collection of location data are misleading or deceptive in breach of section 18(1) of the Australian Consumer Law. We would recommend that this broader issue be considered in the context of Investigation A. To consider this issue, it is useful to extract the relevant statement from Google’s privacy policy in full<sup>10</sup>:

*Your location information*

*We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.*

*Your location can be determined with varying degrees of accuracy by:*

- *GPS*
- *IP address*
- *Sensor data from your device*
- *Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices.*

*The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device’s location on and off using the device’s settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.*

7. This statement may be considered to be misleading and deceptive within the meaning of section 18(1) of the Australian Consumer Law for a number of other reasons. In support of our comments below, we refer to the paper Oracle submitted to the Digital Platform Inquiry initial consultation phase (see <https://www.accc.gov.au/system/files/Oracle-Submission-2-%28September-2018%29.pdf>) which describes the location information that is collected from an Android device.
8. In the context of section 18(1) of the Australian Consumer Law and our paper, the following should be considered:
- (a) The above extract from Google’s privacy policy implies, in the final paragraph, that location information will only be collected if your location setting is turned on. ***This is not correct.*** Google’s privacy policy does not contain any reference to the fact that the Web & App Activity setting on an Android device tracks user location via internet protocol (IP) address and via other activities. An omission of information, particularly where it would be expected to be provided, may constitute misleading and deceptive conduct.
  - (b) Information about the Web & App Activity setting on an Android device is not available under “Location” settings, neither at a device or account level. Instead, users must navigate to “Activity Controls” to see the “Web & App Activity” setting. It is counterintuitive for a consumer to expect that settings governing Google’s location tracking across devices on their account would exist independently of their location settings. Even when that page is viewed, the information that is provided as to the functionality of that setting is not clear and could be considered to be misleading. For example the Location History page states in part: “If you have *other settings like Web & App Activity* turned on and you pause Location History or delete location data from Location History, you *may still have* location data saved to your Google Account ...”

---

<sup>10</sup> <https://policies.google.com/privacy?hl=en-US>

(emphasis added). This is not correct. If Web & App Activity setting is turned on, location data *will* be saved to your Google Account (and will be used by Google). We are unsure of what other settings “like” the Web & App Activity setting will, when turned on, collect the same amount of location data.

- (c) It is not possible, by turning off any settings on an Android device, to turn off all location tracking of that device. In particular, even if location (or Location Services, as it is also known), Location History and Web & App Activity settings are all switched off, the IP address of the relevant Android device will be transmitted to Google. As noted in the extract from Google’s privacy policy above, “your location can be determined with varying degrees of accuracy by ...” IP address. It is misleading not to advise consumers in the privacy policy (or on any other Google page linked to that policy) that it is not possible to stop Google collecting an Android device’s IP address and therefore it is not possible to stop Google collecting some level of location data.
9. We believe the ACCC should consider whether Google’s privacy policy is also misleading and deceptive within section 18(1) of the Australian Consumer Law in the context of the statements made regarding how the location data that is collected by Google is used. The policy states that location information is collected for the innocuous purposes of assisting in allowing Google to offer features like driving directions or movie showtimes. These purposes are not the primary purposes for which location information is collected. Location information (as well as other activity information that Google collects) is primarily collected to sell advertising.

*Other misleading and deceptive conduct that should be included in Investigation A*

10. Our view is that the ACCC should also consider whether other statements that Google makes about the control that a consumer has over his or her data are misleading in 2 respects. First, as to the personal information that Google will actually provide if a consumer seeks to download his or her own data and secondly, as to the accessibility of the data that is held by Google about a consumer. More information is provided on these issues in our separate paper at Attachment A, “Google’s Shadow Profile: A Dossier of Consumers Online and Real World Life”.
11. Google’s marketing promotes the idea that the consumer is in “control” of his or her personal information that Google collects. For example, the first paragraph of Google’s privacy policy states “(w)hen you use our services, you’re trusting us with your information. We understand this is a big responsibility and work hard to protect your information **and put you in control.**”<sup>11</sup> (Emphasis added.) Google states that a consumer’s Google Account will allow that consumer to “(c)ontrol, protect and secure your account, all in one place. Your Google Account gives you quick access to settings and tools that let you safeguard your data and protect your privacy.”<sup>12</sup>
12. Google promises consumers that it is possible to access all of the personal information that Google holds about them via “Google Takeout”, which is accessed from a consumer’s Google Account page headed “Download, delete or make a plan for your data”. Statements at that page of a consumer’s Google Account settings include “Make a copy of your data to use it with another account or service”, “Your account, your data.” and “You can export and download your data from the Google products you use, like your email, calendar, and photos. In a few easy steps, create an archive to keep for your records or use the data in another service.”. However, is not possible to download all of the location data that is collected about a consumer from an Android device from this page.
13. Reviewing network transmission logs from Android devices, there are specific gaps between what a Google Android user’s device collects and the details provided in a user’s Takeout data, including data on nearby Wi-Fi base stations and Bluetooth beacons used to establish location,

---

<sup>11</sup> <https://policies.google.com/privacy?hl=en-US>

<sup>12</sup> <https://policies.google.com/?hl=en-US>

even though this data is directly linked to a Google email address at the time of collection. Google's privacy policy details how Google makes use of data collected from Wi-Fi Access Points, Bluetooth beacons, and even a consumer's IP Address to accurately locate a consumer.<sup>13</sup> Yet when an individual requests their data through the Google Takeout process, Google does not acknowledge or report the Wi-Fi, Bluetooth or IP data collected by Android. This is all important information that a consumer should have, and which it is assumed Google could provide given Google itself uses this data, but the consumer is not provided with this information. This in our view breaches the promise that Google makes to Google Account holders that they are able to control their data (and is a breach of APP 12 as well).

14. Google's privacy policy states that a Google Account holder can review and update the information held about them. Again, this is not correct and in our view this statement is misleading. Google states<sup>14</sup> that a consumer with a Google Account is able to modify his or her interests and choose whether the consumer's personal information is used to make ads more relevant to him or her. However, if a consumer determines *not* to let his or her personal information be used to make ads "more relevant" then that consumer can no longer see the type of inferences that Google has made about that consumer. This does not mean that Google no longer makes those inferences, but simply that the consumer cannot see them. Of course, if a consumer cannot see these inferences the consumer is also not able to change (or, if it wishes to do so, delete) the interests that Google has inferred from that consumer's personal information.

*Action taken in other jurisdictions*

15. In this context, it is also useful to consider a recent first instance French decision of the Tribunal de Grande Instance de Paris in respect of a complaint by the Union Federale des Consommateurs – Que Choisir (a French consumer protection body) against Google. In that decision, which was handed down on 12 February 2019, it was found that a number of Google's privacy policy clauses as in place in 2016 that applied to consumers using Google + (noting these same terms applied to all Google services), were void. Of relevance to the ACCC's investigation regarding misleading and deceptive conduct the French court made the following findings:

- (a) Clause 2 (29 August 2016 version of Google +'s privacy policy) was found to be void. This clause provided: *"Our Privacy Policy explains:*

- *What information we collect and why we collect it.*
- *How we use that information.*
- *The choices we offer, including how to access and update information."*

This is on very similar terms to a clause included in Google's current privacy policy which provides: *"This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information."*

<sup>15</sup>

The French court found that clause 2 was insufficiently clear, complete or detailed as it offered no information regarding the (categories of) recipients of the data shared by Google, the terms of the digital processing carried out by Google and the purposes for which the data was shared, especially in relation to the primary purpose of offering targeted advertising to its users. Despite this clause (together with another clause which is no longer in the policy) serving as a general introduction to Google's privacy policy, the

<sup>13</sup> <https://policies.google.com/privacy?hl=en#infocollect>

<sup>14</sup> <https://policies.google.com/privacy?hl=en-US#intro>

<sup>15</sup> <https://policies.google.com/privacy?hl=en-US>

court found these clauses should have provided essential information, including that the primary purpose of collecting the data was to allow Google to offer targeted advertising to users, which is how Google derives most of its revenues. The clauses were found to be evasive and did not allow the user to understand the actual purposes of the data collection and therefore the extent of the collection of data about him or her and the scope of that consumer's agreement.

- (b) Clause 4 (29 August 2016 version of Google +'s privacy policy) was found to be void. This clause provided: *"We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like."*

This clause is still included in Google's current privacy policy.

For the same reasons as those previously stated in relation to the extracted clause 2 above, the French court found that the way Google portrays the collection of personal data is abusive to the extent it simply presents the collection of data as a way to improve the services offered, whereas the real and primary purpose of this collection is to be able to send advertisements targeted to the same consumer by commercially exploiting his or her personal data.

- (c) Clause 21 (29 August 2016 version of Google +'s privacy policy) was found to be void. This clause provided: *"You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it's important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences."*

This is on very similar terms as a clause included in Google's current privacy policy which provides: *"Browser settings: For example, you can configure your browser to indicate when Google has set a [cookie](#) in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services [rely on cookies to function properly](#), for things like remembering your language preferences."*<sup>16</sup>

The court held clause 21 was intended to dissuade users from blocking cookies, without informing users of the actual scope of the consequences of doing so and was therefore void.

16. In each of the above cases, the French court essentially found that the relevant clauses were misleading in that the clauses did not provide to consumers all of the information that they required to allow consumers to make informed decisions.

#### *Investigation B*

17. Although not stated in the Preliminary Report, we believe that Investigation B may relate to changes made to Google's privacy policy in 2016 that allowed it to combine DoubleClick (as it was then known) data with other personal data collected by Google. We have commented extensively on this issue in our separate paper "Google Stealthily Enables 'Super-Profiles'" at Attachment B and provide our summary comments below.

18. As at 1 May 2012, Google's privacy policy stated:

*We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to*

---

<sup>16</sup> <https://policies.google.com/privacy?hl=en-US>

*share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.*

19. The last sentence of this paragraph had a long history. At the time Google acquired DoubleClick, both regulators and competitors were concerned that Google could combine its already large volume of consumer data with DoubleClick consumer data and raised concerns about the anti-competitive effects of Google doing so. In response to questions of the US Senate Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights, Google maintained that DoubleClick's "*data is owned by the customers – publishers and advertisers – and DoubleClick or Google can't do anything with it*". Likewise, Google told the European Commission that "*the merged entity would also be contractually prevented from using that part of its enlarged database originating from DoubleClick to improve, for example, targeting of search ads on Google's sites or contextual ads in the AdSense network.*"<sup>17</sup> The statement by Google in its privacy policy not to combine DoubleClick data with other data was therefore particularly important as it reflected how Google had agreed to address concerns that had been raised with it by regulators and the assurances that it had given to address those concerns, particularly in light of the fact that since the time of Google's acquisition of DoubleClick it had given itself (via various amendments to its privacy policy) the right to combine other types of consumer data.
20. Concern had been expressed by regulators with the amount of personal information that Google was able to collect and combine, even before Google changed its privacy policy in 2016. For example, the Dutch Data Protection Authority undertook a study in 2013 into Google's practices which raised concerns with Google's then existing practices of combining personal information and resulted in it imposing an up to €15 million fine and requiring changes to Google's privacy policy<sup>18</sup>. Community concerns were also evident, as expressed in this 29 February 2012 Forbes article: <https://www.forbes.com/sites/davidvinjamuri/2012/02/29/did-google-break-the-brand-at-midnight/#45196916663a>. That article raises the topic that is still relevant today and has not yet been adequately addressed:

*There's a very big difference between using data discretely where you find it (like using cookies on web browsers to target advertising based on browsing behaviour) and combining data from different sources. You might be fine with hearing more about cars when you're in the market for one but how about pregnancy, cancer or impotence ...?*

21. The last sentence of the paragraph from Google's privacy policy set out above was removed from Google's privacy policy in June 2016. As pointed out at the time by the US Consumer Watchdog, through this change, "Google finished demolishing the internal firewalls between its vast data-stores, eliminating the last vestige of Internet users' anonymity"<sup>19</sup>.
22. This change to Google's privacy policy to allow it to combine DoubleClick data with the consumer data collected from other sources means Google is now able to combine data from DoubleClick cookies with information from any app or site that uses Google services (including Google Analytics, embedded YouTube video and potentially third party Android apps that use Google's programming interfaces) and with information from Google's own "services" such as Gmail, Google Search, YouTube and the like. This is particularly egregious for the reasons set out below.

---

<sup>17</sup> Google/DoubleClick, para 361.

<sup>18</sup> <https://autoriteitpersoonsgegevens.nl/en/news/cbp-issues-sanction-google-infringements-privacy-policy>

<sup>19</sup> Federal Trade Commission, Complaint Submitted by Consumer Watchdog and Privacy Rights Clearing House in the matter of Google Inc.'s Change in data Use Policies, 16 December 2016.

- (a) Although Google's privacy policy states that it may be updated from time to time, the fact that the undertaking prohibiting the combination of DoubleClick data with other data was inserted to address concerns that had been raised by regulators, which remained as valid in 2016 when the changes were made as in 2007 when DoubleClick was first acquired by Google, would lead a reasonable person to assume that this undertaking would not be changed.
- (b) Google did not explain to consumers, at the time that it made the change to its policy in 2016 to delete the undertaking, the significant impact that this change would have for users. At the time the change was made, existing users had the option to "opt-in", though agreeing to this change was preselected for new users. However, the information provided to assist consumers to determine what they should do referred to the change as necessary to "match" the way people "use Google today" and as providing "new features for your Google account" and did not properly explain the implications of this data combination to users.
- (c) Google still does not clearly explain to consumers the implications for consumers of the collection of DoubleClick data or the combination of that data with other consumer data held by Google. For example, on the Google Search Help page that explains the Web & App Activity setting if the link from the statement "Learn more about [how Google uses your saved activity](#) and helps keep it private" is selected, one is taken to a page that contains no information at all about how Google uses any consumer data (it is necessary to navigate through a further two pages before any such information is provided and, even then, it is very limited, see <https://safety.google/privacy/data/>).
- (d) Google's users were directly harmed by Google's conduct in removing the undertaking from its privacy policy. Insufficient information is given to consumers to allow them to make an informed choice as to whether or not to turn the Web & App Activity setting on or off. Users that do not turn this setting off disproportionately cede control over their data, overpaying Google for the use of Google's services.
- (e) As noted by the Bundeskartellamt in connection with its Facebook decision referred to earlier and in the context of Facebook's practices of collecting and combining data from a number of different sources, the damage to the consumer from these types of practices arises from a loss of control over his or her personal information. A consumer does not know (and cannot easily determine) what personal information is collected and combined or how it is used, particularly in the case of shadow profiling. The same analysis applies to Google and its combination of consumer data with DoubleClick data as applies to Facebook and its collection and combination of data.
- (f) And, finally, it is very difficult for a consumer with a Google Account to determine how to opt out of personalised ads and to opt out of the combination of his or her personal information in connection with the delivery of targeted advertising, as explained in our separate paper "Google Stealthily Enables 'Super-Profiles'" at Attachment B.

23. Therefore there are strong grounds to investigate:

- (a) Whether statements made by Google that it would not combine DoubleClick data with other types of data (including in its privacy policy) amount to misleading or deceptive conduct under section 18 of the Australian Consumer Law.
- (b) Whether statements made by Google to consumers when it amended its privacy policy to allow it to combine DoubleClick data with other consumer data (and the statements currently available from various Google Account and Google help pages dealing with the same issue) amount to misleading or deceptive conduct under section 18 of the Australian Consumer Law.



- (c) Whether amending Google’s privacy policy to allow the combination of DoubleClick data amounts to unconscionable conduct for the purposes of section 21 of the Australian Consumer Law, given the context in which it occurred including previous undertakings not to do so and Google’s failure to adequately explain to consumers the significant impacts of the change to its privacy policy.
- (d) Whether the provisions of Google’s privacy policy that allow it to combine DoubleClick data are unfair contract terms for the purposes of section 23 of the Australian Consumer Law. Our view is that these provisions are unfair contract terms, as they create a significant imbalance between the rights and obligations of the parties (Google obtains the ability to create a super profile of the consumer which it is able to monetise but the consumer receives a benefit of a lesser value, being the right to use Google’s services and in addition loses the ability to control his or her online privacy), the ability to combine this data is not necessary to protect Google’s legitimate interests and significant detriment to a consumer occurs as a result of his or her loss of control of privacy. And, finally, there is a lack of transparency in the terms of the privacy policy and Google’s general terms and conditions which significantly impedes the exercise by consumers of the limited rights that they do have to opt out of targeted advertising and the combination of their personal information in connection with such targeted advertising (which are only available to those Australian consumers with a Google Account in any event).

#### *Investigation C*

- 24. Investigation C, which we understand is an investigation generally into whether digital platforms’ consumer terms of use and privacy policies may contain unfair contract terms under the Australian Consumer Law, is an important investigation in relation to Google. The following comments focus specifically on Google’s privacy policy and terms and conditions in this context.
- 25. We believe that, if Google’s privacy policy and terms of use are examined through the lens of the unfair contract terms provisions of the Australian Consumer Law, those terms that require users to agree to the collection and *combination* of disproportionate amounts and detail of user data in order to use Google’s ubiquitous services would be found to be unfair (and therefore void). We have already commented on this in the context of the provisions of Google’s privacy policy that allow it to combine DoubleClick data and other data.
- 26. The “take it or leave it” nature of Google’s privacy policy would also, in our view, be found to be unfair (and therefore void) under the Australian Consumer Law. As noted throughout the Preliminary Report, consumers who are uncomfortable with the amount of data that Google is able to collect about them feel they have little choice but to agree to that data collection, given that there are no alternative third parties services available to replace many of Google’s ubiquitous services.
- 27. Google has the right to unilaterally change its privacy policy. The ACCC’s public guidance on the unfair contract terms regime suggests that in some cases a clause which provides a unilateral right to amend a contract will be an unfair contract term. This should be considered to be one of those cases – there is really very limited choice for a consumer to reject an amendment made by Google to its privacy policy as this would mean Google’s services could no longer be used by that consumer even after they have been locked in to these services in various ways. As noted earlier, even consumers who are uncomfortable with Google’s privacy policy and terms and conditions feel they have little choice but to accept them given the lack of substitutable services.
- 28. Transparency is relevant to determining whether a term is unfair. Google’s privacy policy and its terms and conditions are not transparent. The Preliminary Report refers to the lack of transparency of digital platforms’ data practices and the concerns that have been expressed by consumers regarding this lack of transparency. Looking at Google’s privacy policy and its terms

and conditions, it is difficult for a consumer, whichever of Google's services he or she uses, to work out what data he or she is providing to Google, how to take steps to limit that data collection and how to stop Google storing and using that data (including by combining data for the purposes of creating super profiles). For example:

- (a) As referred to elsewhere, the statements made in the privacy policy regarding the collection of location data and what Google may do with it and also the statements regarding the combination of data which Google obtains from different sources to create super profiles, which a consumer is agreeing to when it agrees to Google's privacy policy are not transparent (and in fact at least in the case of location data are misleading).
- (b) It is very difficult for consumers to determine how to effectively "amend" the agreement with Google to limit the types of consumer data that Google collects, or to limit the use which may be made of that data, by adjusting different settings. Again, we refer to the paper we submitted to the Digital Platform Inquiry initial consultation phase (see <https://www.accc.gov.au/system/files/Oracle-Submission-2-%28September-2018%29.pdf>) and our new paper, "Google Stealthily Enables 'Super-Profiles'", which is in Attachment B, which demonstrates the difficulties encountered by consumers in first, determining what settings need to be adjusted to limit the collection of location data (as well as other data) and, second, how to actually access and adjust those settings.

29. The ACCC's investigation appears intended to consider the unfair contract terms provisions only in the context of the consumer. At page 237 of the Preliminary Report it is noted:

*Due to the significant information asymmetries and bargaining power imbalances in the relationship between consumers and digital platforms, consumers are unable to negotiate a fair bargain with digital platforms for the collection, use and disclosure of their personal data. This bargaining imbalance results in terms within the consumer bargain that are potentially unfair contract terms (UCTs) under the ACL.*

30. The terms and conditions that Google imposes on its true customers that it cares commercially the most about, the purchasers of its adtech services, would also fall within the unfair contract terms regime where Google's customers are small businesses. Exactly the same comments as extracted above could be made in relation to the contractual arrangements between Google and such small business customers. In fact, given the significant market position of Google, the same conclusions could be reached in relation to *any* business that uses Google's adtech services, however large. Indeed, the UK Cairncross review concluded that, because of its position, Google (and Facebook) can impose terms on publishers without the need to consult or negotiate with them. The review found that the bargaining imbalance is so pronounced that this could threaten the viability of news publishers' online businesses.<sup>20</sup>
31. Attachment C sets out in detail a number of the clauses from Google's standard form advertising services contracts which, in our view, are clearly unfair contract terms. The ACCC has already found that clauses in advertising contracts that are to the same effect as some of the Google clauses will be unfair. In this regard we draw the ACCC's attention to the following, as set out in the ACCC's publication "Unfair terms in small business contracts: A review of selected industries November 2016" (**Unfair Terms Publication**)<sup>21</sup>:

---

20

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/778021/021119\\_THE\\_CAIRNCROSS\\_REVIEW\\_A\\_sustainable\\_future\\_for\\_journalism.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/778021/021119_THE_CAIRNCROSS_REVIEW_A_sustainable_future_for_journalism.pdf) (see Chapter 4).

21

[https://www.accc.gov.au/system/files/B2B%20UCT%20-%20Final%20-%20Unfair%20terms%20in%20small%20business%20contracts%20%20A%20review%20of%20selected%20industries\\_0.PDF](https://www.accc.gov.au/system/files/B2B%20UCT%20-%20Final%20-%20Unfair%20terms%20in%20small%20business%20contracts%20%20A%20review%20of%20selected%20industries_0.PDF)



- (a) The ACCC found terms that allowed unilateral variation to an advertising contract could be unfair, particularly where these gave the publisher the ability to vary the product offering or price and the advertiser did not receive prior notice and was not given the opportunity to terminate the contract once the change had taken effect. To remedy the ACCC's concerns, one digital publisher amended its standard form contract so that it is required to provide advertisers with at least 7 days' notice of material changes to its terms. As noted in Attachment C, Google has the right to unilaterally vary its terms without providing any notice at all to its business customers (see section A).
  - (b) The ACCC provided as an example of an unfair contract term in an advertising contract one that allowed a publisher to remove content without prior notice to the advertiser and for any reason. The ACCC required the publisher to amend the term so that it could only remove an advertisement in limited defined circumstances, including if the advertisement contravened any law, was likely to infringe on the rights of third parties or was obscene or defamatory. As noted in Attachment C, Google may remove ads "at any time for any or no reason"<sup>22</sup>.
  - (c) The ACCC commented adversely on standard form contracts that allowed the publisher to terminate for any breach of the contract, regardless of how trivial. It noted that broad, unrestrained termination clauses are likely to be unfair. Google may terminate accounts for any reason (which is the equivalent of terminating a contract), as demonstrated by the clauses set out in section C of Attachment C, with a business customer typically having very limited rights to appeal such a termination, as set out in section D of Attachment C.
32. Finally, as noted previously, the unfair contract terms regime requires consideration to be given to the "transparency" of a term. The ACCC has commented extensively on the lack of transparency in Google's privacy policy and consumer terms and conditions in the Preliminary Report. This lack of transparency is even more apparent in the context of Google's advertising services terms and conditions, as referred to in Attachment C. For example, as noted in paragraph A.1 of Attachment C, a requirement for business customers to comply with "our policies" requires compliance with 23 separate policies – and compliance requirements are not limited to those policies in any event. The business customer must also comply with "any other policies" made available by Google. In each case, Google has the unfettered right to amend these policies in its absolute discretion.
33. The clauses listed in Attachment C are by no means the only problematic terms included in the extensive range of terms and conditions and policies that are required to be complied with by any business that uses Google's adtech related services. For example, Google's Advertising Program Terms contain broad indemnities from business customers<sup>23</sup>, while Google itself has the benefit of a very wide release of liability<sup>24</sup>, which the Unfair Terms Publication considers to be problematic under the unfair contract terms regime.
- The ACCC has, in the past, taken action regarding:
- (a) Uber: requiring it to amend the clause of its standard driver agreement that allowed Uber to terminate the agreement without cause; and
  - (b) Fairfax Media: requiring it to amend its advertising contract that allowed it to refuse or withdraw a customer's advertisement for any reason at any time.
34. It is recommended therefore that the ACCC give careful consideration to Google's standard form business contracts in the context of the unfair contract terms regime and in light of its focus on

<sup>22</sup> [https://payments.google.com/payments/apis-secure/get\\_legal\\_document?ldi=30847](https://payments.google.com/payments/apis-secure/get_legal_document?ldi=30847)

<sup>23</sup> See clause 11 here: [https://payments.google.com/payments/apis-secure/get\\_legal\\_document?ldi=30847](https://payments.google.com/payments/apis-secure/get_legal_document?ldi=30847)

<sup>24</sup> As above, see clauses 9 and 10.

enforcement of this regime. Not only would this result in positive changes to Google's business standard form contracts but it would also act to provide guidance for other digital platforms.

**D. Areas for further analysis**

1. The ACCC has requested further submissions in relation to (amongst other matters) the following:
  - (a) *Deletion of user data*: The ACCC has asked for views on whether there should be an explicit obligation to delete all user data associated with an Australian consumer once that user ceases to use the digital platforms services or whether user data should automatically be required to be deleted after a set period of time.
  - (b) *Prohibition against unfair practices*: The ACCC is seeking views on whether the CCA should be amended to include a general prohibition on unfair practices, similar to section 5 of the US Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices in or affecting commerce.
2. Oracle is pleased to provide the comments below in relation to these issues.

*Deletion of user data*

3. The Preliminary Report seeks views on whether digital platforms should be required to delete all "user data" either after a consumer ceases to use that platform's services or after a fixed period of time.
4. Again, we support this proposal and wish to raise a few additional points:
  - (a) In this context "user data" should be given a broader meaning than "personal information" as defined in the Privacy Act. The definition should be broad enough to cover all data that is collected by a digital platform and linked to an account or device ID of that consumer given that Google uses this data to create detailed super profiles of consumers. This will ensure that the operation of the prohibition is not avoided by complex legal arguments as to what is, or is not, when considered in isolation, personal information.
  - (b) We again draw attention to the difficulties of determining when a consumer is using a platform's services, particularly in the case of Google, given Google will collect a consumer's personal information in a broader range of circumstances than may be expected, for example, simply when a consumer visits a website that uses Google Analytics (see our previous discussion of this topic). To avoid the need to analyse when a consumer is or is not using such services, the new regulation should prescribe that deletion would be required to occur automatically at fixed intervals. To avoid consumers being disadvantaged by this, it should be possible to allow for consumers to expressly (and on the basis of very clear and informed consent) opt-out of such deletion occurring. Platforms should be prohibited from providing any form of incentive to consumers (or coercion of consumers) to opt-out of such data deletion.

*Prohibition against unfair practices*

5. Section 5 of the US Federal Trade Commission Act provides the Federal Trade Commission (**FTC**) with enforcement authority over "unfair or deceptive acts and practices". These two terms, "unfair" and "deceptive", are broad and have been defined through case law rather than through statute. This has been by design. Allowing the US Courts to draw the lines of impermissible conduct has allowed the authorities of the FTC to evolve with the marketplace, consumer expectations and technology.
6. For a consumer injury to be "unfair" under section 5 it must meet a three part test. First, the injury must be "substantial". Substantial injury could be a large harm to a small amount of

consumers or a small harm to a large set of consumers.<sup>25</sup> Second, the action must be unavoidable. As the FTC has explained, “Normally we expect the marketplace to be self-correcting, and we rely on consumer choice - the ability of individual consumers to make their own private purchasing decisions without regulatory intervention - to govern the market. We anticipate that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory.”<sup>26</sup> Finally, the harm at issue cannot be outweighed by a corresponding benefit in the marketplace or to consumers. The “net effects” of the practice must be negative.

7. In the FTC context, a central element to unfairness is the inability for consumers to avoid the harm. As the ACCC notes in the Preliminary Report, Google’s privacy policies have a strained understanding of “consent” in how they are presented to consumers. The analogy used by the Commission is to compare them to click wrap agreements, which were once common with software purchases. In the platform services context, the click wrap agreements contain the parameters of the data collection often in highly dense, hard to read language, and are paired with the offer of a “free” service in exchange for a click agreement. As the ACCC notes, this preys on the behavioural biases of the typical consumer.
8. Recognising this, the FTC has used this behavioural inclination to determine unfairness. In the *Federal Trade Commission v Commerce Planet*<sup>27</sup> case a charge of unfairness was brought even though the underlying conduct was spelled out in the terms and conditions of the service. Commerce Planet was a business that purported to sell online auction kits to help optimise earnings for clients on online marketplaces. Consumers who landed on the Commerce Planet website were enticed to buy the online selling kit. The various click agreements had links to privacy practices and a “Terms of Membership” agreement.
9. It was only on the “Terms of Membership” agreement page that consumers were informed that enrolling in the program meant signing up for an expensive negative option subscription plan. Because this notice only appeared buried on a web page most consumers would never have the wherewithal to reach, or read if they did reach, the FTC found this to be “unavoidable” for consumers. Quite simply, a consumer could agree to the abusive terms without ever actually seeing them.
10. In 2017, the FTC used section 5 to stop Vizio, a manufacturer of high-definition televisions, from obfuscating consumer privacy choices in its sets’ set up menus. In *Vizio*, the FTC alleged that the company masked privacy settings behind set-up menu choices that provided consumers with limited understanding of their data sharing options. Vizio’s technology allowed the company to track the pixels appearing on a consumer’s television. This tracking allowed for a minute-by-minute accounting of a person’s viewing habits. The FTC found that the notice and choice offered by the company was faulty. Privacy choices were provided in the set’s “Smart Interactivity” menu, and consumers were only told that their opting in would allow for program recommendations to be made. They were not made aware of the pixel tracking or that the data derived from it would be sold to advertisers, marketers, and data brokers
11. The broad authorities against “unfair or deceptive acts and practices” also allowed for the FTC to examine the source code underlying the apps running on smart phones. In 2016, the

<sup>25</sup> There is currently a vigorous legal debate as to whether there needs to be an economic nexus as well. Privacy violations and data security breaches are often challenging to assess definite financial damages. For instance, due to the frequency and growing scale of data hacks, victims of identity theft might have difficulty confidently assessing causality to any single breach. Similarly, an abrogated privacy policy might result in more online marketing, but not any recognised financial impact.

<sup>26</sup> *FTC Unfairness Statement*, found at <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>

<sup>27</sup> *FTC v. Commerce Planet*, found at <https://www.ftc.gov/sites/default/files/documents/cases/2009/11/091119complanetcmpt.pdf>

Commission settled a case with InMobi, a company that billed itself as “the largest independent mobile ad network”. App developers used InMobi’s software development kit in their applications in order to receive ads to monetize their apps. InMobi’s technology allowed for the geotargeting of ads. The FTC found, however, that InMobi’s geotargeting occurred even if a consumer disabled location tracking on their phone. The FTC found that this digital conduct adhered to its century old unfairness and deception authorities.

12. Although the FTC’s use of section 5 has not been free of criticism, it has proved to be robust, principles based regulation that is well adapted to deal with changing technologies in various different markets.

#### **Additional points**

1. Oracle wishes to raise two other matters in this submission, in relation to:
  - (a) *The definition of “personal information” for the purposes of the Privacy Act:* The Preliminary Report raises the question of whether location data would be personal information under the Privacy Act.
  - (b) *Emerging competition in data collection:* Chapter 7 suggests that the monopoly Google currently has in relation to the collection of personal information is likely to be challenged in the near future.
2. We offer the comments set out below in relation to each of these issues.

*What is “personal information”?*

3. Section 5.6.1 of the Preliminary Report states:

*It is not clear whether the scope of ‘personal information’ under the Privacy Act includes metadata such as IP addresses, other location data, or other technical data.*

4. We do not believe the recent decision in Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (**Grubb’s case**), which is referred to in the Preliminary Report, suggests that location data is not personal information under the Privacy Act.
5. Grubb’s case considered the scope of personal information in the context of a request from Mr Grubb to Telstra Corporation Limited (**Telstra**) for access to so called metadata stored in relation to his mobile phone service. Although Grubb’s case concerned an earlier definition of personal information and a request for access to information under the then applicable National Privacy Principles, the Federal Court’s comments on the interpretation of personal information continue to have relevance to the Privacy Act as it now is.
6. In particular the Federal Court looked at the requirement that the information or opinion be “about an individual” in the context of the request that Mr Grubb had made. At paragraphs 63 and 64 of the judgement it was made clear that the individual must be a subject matter of the information (or opinion, as applicable). Specifically, it was noted:

63. *The words “about an individual” direct attention to the need for the individual to be a subject matter of the information or opinion. This requirement might not be difficult to satisfy. Information and opinions can have multiple subject matters. Further, on the assumption that the information refers to the totality of the information requested, then even if a single piece of information is not “about an individual” it might be about the individual when combined with other information. However, in every case it is necessary to consider whether each item of personal information requested, individually or in combination with other items, is about an individual. This will require an evaluative conclusion, depending on the facts of any individual case, just as a*

*determination of whether the identity can reasonably be ascertained will require an evaluative conclusion.*

64. *In some instances the evaluative conclusion will not be difficult. For example, although information was provided to Mr Grubb about the colour of his mobile phone and his network type (3G), we do not consider that that information, by itself or together with other information, was about him. In other instances, the conclusion might be more difficult. ...*

7. The location and other mobile data collected by Google is quite different to the data that was the subject of the dispute in Grubb's case. This location and other mobile data is clearly personal information – streams of user location (including activity) data from Android smartphones create detailed profiles of real-world behaviour of individuals and their patterns of life – a second-by-second record of an individual's every movement is highly personal. Furthermore, it is clearly linked directly to a particular individual (where the location information is retained with the device user's Google Account) or to an individual whose identity is reasonably able to be determined, given the data is associated with unique identifiers where it is not associated with the user's Google Account.

8. Freelancer International Pty Ltd and Australian Information Commissioner [2017] AATA 2426 (**Freelancer**) is not referred to in the Preliminary Report, but it is also useful to consider that decision in this context. Freelancer is also distinguishable. Of relevance, that Administrative Appeals Tribunal (**AAT**) decision considered the question of whether an internet protocol (**IP**) address was personal information. It was held that it was not. Although, again, the decision considered the pre-March 2014 legislative regime, the comments of the AAT remain relevant in interpreting the Privacy Act, as it now is. As noted at paragraph 63 in the decision:

63. *An IP address received in the manner typical of activities involving visits to Freelancer's website does not merit characterisation of the IP address as being "about an individual". Neither does it merit characterisation as being information from which an individual's identity can reasonably be ascertained. This is so because of the inherent characteristics of IP addresses and the practices involved in their allocation and use. ... any particular user's recorded IP address may change over time, and do so in apparently idiosyncratic fashion. It may also stay the same, over significant periods of time. But because the recorded IP address is only that of a network interface device (including potentially, the address of a "proxy server") there is no way of discerning either the use of any particular terminal device, or an individual's identity, from an IP address.*

9. Location and other mobile data is in a different category to an IP address collected in isolation – it is both information or an opinion about an individual and it is also information from which, when considered in light of the information with which it is associated by Google (that is, a user's Google Account and/or other unique identifiers), information about an identified individual or an individual who is reasonably identifiable. Some location data is derived through device identifiers (of which an IP address is but one).

10. In short, even race, age, health, religion and financial status may be deduced from the places a person's smartphone frequents. For example, tracking a user's location over time can reveal whether, how frequently and which religious services the user attends, consults medical professionals, attends political gatherings and/or frequents LGBTQ establishments, and where the user spends his or her nights and waking hours. Therefore it is clear that the location and other mobile data collected and used by Google is personal information (and may well be sensitive information) for the purposes of the Privacy Act.

### *Future trends*

11. We also wanted to comment on certain of the future trends that have been identified in Chapter 7, specifically in relation to:
  - (a) emerging technologies and advancements in data use, security and authentication; and
  - (b) potential changes to the composition and function of major digital platforms, including the entry and exit of market participants.
12. The Preliminary Report suggests:
  - (a) The ever-increasing popularity of Internet of Things (**IoT**) devices has allowed, and will continue to allow, potentially aided by the introduction of 5G technology, increased data collection from consumers. The ability to create highly detailed profiles of consumers through the collection and combination of such vast quantities of data has the potential for both positive and negative outcomes, some of which are highlighted in the Preliminary Report.
  - (b) There is the possibility of dynamic changes in relevant markets that will see the entry of new digital platforms and the exit of some digital platforms from relevant markets, though the Preliminary Report also notes the possibility that Google (and Facebook) could foreclose competition in specialised search services markets.
13. Although markets for the supply of online search services, social media services and related digital platform markets are subject to ongoing change, this of itself does not mean that these markets are competitive or that there is the potential for new platforms to emerge that may become dominant. It also does not mean that competitive dynamics will ensure that consumers' rights to privacy, or to prevent exploitation of their data, will be protected.
14. It is not realistic to expect that in the short or medium term there would be any competitor to Google who would be able to create the same detailed super profiles of consumers as Google has been able to create (and continues to develop). In particular, we draw your attention to the following:
  - (a) Google collects personal information through Google Search (which is used 6 billion times per day), the Android operating system (which is installed on approximately 40% of mobile devices in Australia), its ad tech products (present on over 80% of internet websites) and from its widely used applications such as YouTube and Google Maps. Therefore it is able to collect personal information from consumers from a vast range of sources.
  - (b) Not only does Google collect personal information from all of these different sources but it *combines* this data (including data that is collected from different devices). This is expressly permitted by its privacy policy. There are also no settings or other adjustments that may be made by a Google Account holder (or any other consumer in respect of whom Google collects data) that would impose a restriction on Google's ability to *combine* the data that it has collected (though changes may be made to device settings to limit the data that is collected).
  - (c) Google is able to collect data not only from consumers that hold Google Accounts (whether or not any such consumer is signed in to the relevant account) but also from other consumers. That is, a consumer that does not have a Google Account and is not directly using a Google service such as Google Maps or YouTube will still provide his or her data to Google if that person visits a website that uses Google's services, such as Google Marketing Platform (formerly DoubleClick) cookies or Google Analytics. Therefore, not only is a vast amount of data collected and combined but it is collected from a vast number of individuals.

15. Given that Google has collected, and combined, personal information from consumers over a long period of time, it has created a “data moat” that constitutes an enormous and insurmountable barrier to entry and expansion of Google’s competitors in the online search advertising markets and ad tech intermediary markets.
16. Competitors are unable to come anywhere close to collecting and combining sufficient data to allow them to create similarly accurate and detailed super profiles of consumers to those that Google is able to create – no matter how much they invest and try to innovate. Such competitors cannot compete with Google in online search advertising markets, or in any ad tech intermediary markets, because they cannot offer ad targeting of a similar quality to Google. As a consequence, Google’s data moat limits the likelihood that any serious competitors to Google will emerge in these markets, at least in the short to medium term. This data moat also means there is no incentive for Google, absent regulatory intervention, to take serious steps to protect the privacy of consumers or to cease exploiting the data it collects.
17. As demonstrated in the Preliminary Report, not only is Google at the forefront of the provision of existing services and technologies that are used for the collection of consumer data, but is also at the forefront of the new technologies used for IoT devices and the provision of IoT services. Therefore even the further development of those markets as IoT usage becomes more popular will not mean that Google’s current monopoly position in online search advertising markets is subject to serious challenge.

## **Oracle Corporation**

1 March 2019

ATTACHMENT A  
**Google's Shadow Profile:**  
**A Dossier of Consumers Online and Real World Life**  
*February 2019*

**Executive Summary**

*A consumer sees an ad that is unnervingly, pointedly accurate. It seems to target information – so personal, so specific – that only this consumer would know the information. Maybe the ad targets a secret interest or hobby, a special place, or intimate lifestyle details. Is the microphone on? Is the camera activated? No –but they might as well be. In fact, Google is using massive amounts of consumer data, not all of which it discloses to consumers, to micro-target advertising. All without the consumers knowledge or consent.*

Google's corporate mission is "to organize the world's information and make it universally accessible and useful." What it does not widely acknowledge is that this mission is as much about collecting data as it is about categorizing information. Google acknowledges certain data collection activities, and even purports to grant consumers control over what is collected and how it is used. However, the scope and extent of Google's data collection extends far beyond what is acknowledged or widely known, and its controls fail to address most of this data. As a result, consumers cannot fully understand – much less control – all of the data that Google holds on them.

While Google touts "improved" consumer control over the data it collects (as a result of the EU's General Data Protection Regulation), this is misleading. A close reading of Google's statements and policies indicates the company does not disclose the full extent of the information it collects on consumers, nor the valuable inferences it draws from this data. Analysis of communications from an Android smartphone suggests Google keeps hidden far broader profiles on billions of consumers around the world – removed from individual view or access, and public accountability. For example Google's "My Activity" page contains a history of what the consumer viewed, searched for, and browsed.<sup>1</sup> However, it *omits* much of the data the company collects, which is often far more invasive and revealing.

This *omitted* data is a consumer's "shadow profile" – massive, largely hidden datasets of online and offline activities. This information is collected through an extensive web of Google services, which is difficult, if not impossible to avoid. It is largely collected invisibly and without consumer consent. Processed by algorithms and artificial intelligence, this data reveals an intimate picture of a specific consumer's movements, socio-economics, demographics, "likes", activities and more. It may or may not be associated with a specific users' name, but the specificity of this information defines the individual in such detail that a name is unnecessary.

Google offers a "Takeout"<sup>2</sup> page that purports to offer a complete view of the data Google collects on a consumer. Consumers can download a file including "Takeout data," which

---

<sup>1</sup> <https://myactivity.google.com>

<sup>2</sup> <https://takeout.google.com>



includes the content that Google scans to infer personality and interests, such as emails, interactions with other consumers, ad clicks, location, uploaded documents, and physical activity data. However, this file, which can contain years of personal information, omits *entire categories* of other data collected by Google.<sup>3</sup> While purporting to provide a complete picture of the data Google holds on a consumer, it is only a fraction of Google's actual online tracking.

Notably, "Takeout" data excludes a consumer's interest profiles, the most critical information that Google stores. Google only shows users the interests that it ascribes based on their personal data *if the consumer elects to see personalized ads* from Google. Yet Google's data set is so immense and its collection so pervasive that it can profile the interests of, and deliver ads to, consumers who have "opted-out" or deleted their data *just as effectively* as it can consumers who remain inside Google's ecosystem. This information is not included in "Takeout" data, leaving consumers in the dark.

Furthermore, the Takeout service only works for consumers who have a Google Account. Consumers who are *not signed into, or do not even have*, a Google Account may still have data collected on them and remain subject to Google's privacy policy and terms of service. A consumer visiting a website using Google Analytics is automatically subject to Google's privacy policy (data collection policies), allowing Google to collect unique identifiers on their device, their location, "cookie" data and metadata. None of this data is accessible or known to the consumer.

This data collection keeps Google in business. Google directly monetizes both "Takeout" and "shadow profile" data through digital advertising. For example, in communications to advertisers and publishers, Google highlights their ability to target ads based off Internet Protocol (IP) Address. Google also admitted that it *infers demographic data* from a consumer's IP Address.<sup>4</sup> Google tells advertisers it is able to tie this profile to consumers via cookies.<sup>5</sup> As a result, in 2018, Google's advertising revenue totaled \$116 billion, or 85% of its total. The more data Google collects on consumers, the better it can target ads and the more money it makes.

## Google's Android Data Collection Platform

One of the most *invasive and pervasive* tools in Google's data collection arsenal is the Android smartphone. Smartphones are so integrated in consumers' everyday life that it is literally an extension of a consumer's personality. For sure, a smartphone is a phone, a calendar, a web browser, a music player, a camera and an access point for social media, but it is also an invasive tracker of health, precise movements, location, interests, and places frequented. Further, smartphones are also surveillance tools for Google to collect important information about one's physical environment, such as nearby Wi-Fi base station or Bluetooth beacons, in both public

---

<sup>3</sup> Including people's webpage interactions, ad interactions, device sensor data (eg: from their Android phones), search results clicked, Chromecast usage data, Google Docs keywords, Email keywords, and social graph.

<sup>4</sup> Letter from Google to US Senate (Page 5, Paragraph 3)

<https://www.blumenthal.senate.gov/imo/media/doc/05.11.2018%20-%20FTC%20-%20Google%20Location%20History.pdf>

<sup>5</sup> <https://support.google.com/google-ads/answer/2580383?co=ADWORDS.IsAWNCustomer%3Dfalse&hl=en>

and private places. Google not only constantly tracks the location of Android users, but also links the data collected by an Android smartphone to unique device and account identifiers. (Table 1)

Unique Identifier	Description	Scope
Name and Email Address	Individual's ID and user name in the Google ecosystem	Account
Advertising ID	ID for advertising, provided by Google Play Services	
Android Certificate	Signifies a Google account on a device is verified <sup>6</sup>	
International Mobility Equipment Identity (IMEI)	Universal hardware identifier for mobile phone	Device
Media Access Control (MAC)	Hardware identifier for devices on a network	
Internet Protocol (IP) Address	Every device connected to the internet is assigned an IP address <sup>7</sup> ; can be used to establish a device's location	
Serial Number	A manufacturer specific hardware identifier	

Table 1: Unique Identifiers Associated with Devices and Google Accounts

One particular Google service on Android smartphones – “checkin” – ties together many unique identifiers Google collects about a consumer and their device(s). With this data Google can readily combine multiple sets of data into a large super profile of a consumer. For example, Google’s Android tracks a mobile phone’s unique IMEI, linking it in the same file communicated to Google’s servers to account identifiers such as an Android ID, (Figure 1) which begs the question whether is it more important to know a consumer’s name or their unique set of IDs.



	<div>conv ID</div> <div>test name</div> <div>phone</div> <div>host</div> <div>api</div> <div>src file</div> <div>timestamp</div>	<div>621864</div> <div>0107WeatherChannelTest</div> <div>Sony Xperia A</div> <div>android.googleapis.com</div> <div>checkin</div> <div>2019-01-16 14:00:05</div>
	<div>— from req —</div> <div>imei</div> <div>wifi_mac</div> <div>android_id</div> <div>email/acct</div>	<div>357008084578329</div> <div>84c7ea832819</div> <div>3ff08958e43ca784</div> <div>[andrea.x.test@gmail.com]</div>
	<div>— from req —</div> <div>model</div> <div>device</div> <div>serial</div> <div>fingerprint</div> <div>manufacturer</div>	<div>G8142</div> <div>G8142</div> <div>CB512F35YH</div> <div>Sony/G8142/G8142:8.0.0/4...</div> <div>Sony</div>

Figure 1: Example Data elements reported by Google Android via “CheckIn” service

<sup>6</sup> <https://developers.google.com/android/guides/client-auth>

<sup>7</sup> <https://policies.google.com/privacy?hl=en>

Reviewing network communications between an Android phone and Google servers, at least four different types of identifiers are transmitted, collecting at least 18 different data elements. (Table 2) Google combines the data it collects about account and device identifiers with accurate and specific location information of a consumer. Location data linked with an Android ID and/or other unique identifiers including a consumer's Google account is personally identifiable. Over time, this data creates a detailed profile about a consumer; where they live, work, shop, eat, socialize with, and many other revealing insights about their pattern of life, for Google's use in providing detailed advertising profiles.

Type of Data	Data Elements Collected
<b>Device Identifiers</b>	Make, Model, Manufacturer, Android Version
<b>Unique Device Identifiers</b>	Serial Number, International Mobility Equipment Identity (IMEI), Media Access Control (MAC) Address, Internet Protocol (IP) Address
<b>Google Account Identifiers</b>	Email Address, Android ID, Advertising ID
<b>Location and Environment</b>	GPS, Wi-Fi Access Points, Bluetooth Beacons, Barometric Pressure, Activity Readings (Motion Sensors)

Table 2: Key Data Types and Elements Collected by Google Android

Through constant tracking of consumers in the physical world and on the internet across various devices, Google is able to create a virtual dossier on nearly every internet user for the purposes of digital advertising and developing new products and services. The myriad of app level, device level, account level collection, combined with numerous *redundant* ID's creates a cat and mouse game where consumers – even the most sophisticated consumers – reveal far more data than they intend. Google's vast data set on consumers is critical to its ability to generate revenue via advertising.

### Data Missing from Google Takeout

Google claims consumers have control of their data via Google Takeout, a service available to Google Account holders to “create an archive with your data from Google products.”<sup>8</sup> As stated above, the data Google makes available to consumers through this process is a limited portion of the larger super-profile that Google maintains on consumers. (Table 3) As evidenced by network transmission logs from Android devices, there are specific gaps between what a Google Android user's device collects and the information Google reveals in a consumer's Takeout data. Missing data includes information on nearby Wi-Fi base stations and Bluetooth beacons used to establish location, despite the fact this data is directly linked to a Google account at the time of collection. This missing information provides essential data for Google's “shadow profile” on consumers.

<sup>8</sup> <https://takeout.google.com/settings/takeout>

Location Data Element	Collected by Google?	Tied to Unique Identifier?	Type of Unique Identifier	In Takeout?
GPS Coordinates + Accuracy	YES	YES	Android ID	YES
Altitude	YES	YES	Android ID	YES
Wi-Fi Scans	YES	YES	Android ID	NO
• MAC Address	YES	YES	Android ID	NO
• Signal Strength + Frequency	YES	YES	Android ID	NO
Bluetooth Beacon Scans	YES	YES	Android ID	NO
• MAC Address	YES	YES	Android ID	NO
• Signal Strength + Frequency	YES	YES	Android ID	NO
Cell Tower Readings	YES	YES	Android Cert	NO
Barometric Pressure Readings	YES	YES	Android ID	NO
Activity Readings + Confidence Level	YES	YES	Android ID	NO
Source of Location Reading (Cell or Wi-Fi)	YES	YES	Android ID	NO
Connection to Wi-Fi Access Points	YES	YES	Android ID	NO
IP Address	YES	YES	Various	NO
PlaceIDs	YES	YES	Android Cert	NO
Rate + Change in Rate of Collection	YES	YES	Android ID	NO

Table 3: Data Missing From Google Takeout

Google's Privacy Policy details how Google makes use of data collected from Wi-Fi Access Points, Bluetooth Beacons, and even a consumer's IP Address to accurately locate a consumer.<sup>9</sup> To collect this data, *Google opts consumers into* extensive location tracking by default (Figure 2) when creating an account. Yet when an individual requests their data through the Google Takeout process, Google does not acknowledge or report the Wi-Fi, Bluetooth, and IP address data that Google collects.

<sup>9</sup> <https://policies.google.com/privacy?hl=en#infocollect>

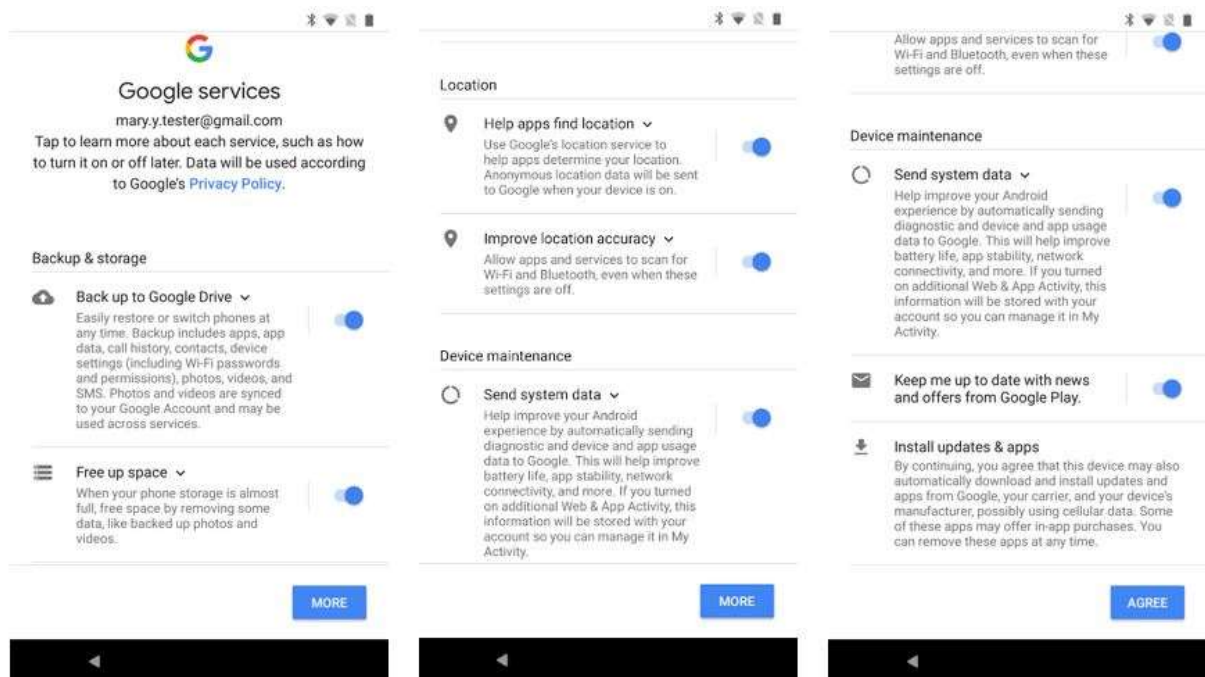


Figure 2: Screenshots of Google Services Defaults During Android Device Setup

For example, in the Location History file contained within the Takeout documents provided to a consumer, Google reports a list of GPS Coordinates and altitude readings accompanied by an accuracy range of that location in meters and timestamp. (Figure 3) While this information is some of the data Google collected about the device, it is not a comprehensive list of the location data and metadata associated with a consumer.

Figure 3 compares the information presented to the consumer from Google's Takeout documents, with a copy of the network communication to Google servers from the same Android device during this same time period. While Google collects, scans, and stores barometric pressure readings, Wi-Fi base stations and Bluetooth beacons via Android devices to determine the location of a consumer,<sup>10</sup> it does not make that data available, even though the information is directly tied to a consumer's Google Account. Figure 3 reveals details on the location event recorded by an Android device via a Wi-Fi Scan, yet in the Takeout documents Google does not reveal the source of location or the list of Access Points used to pinpoint the location.

Location information is valuable to Google for the purposes of targeted advertising. Exact GPS coordinates are a very precise way to locate a consumer, but GPS is both taxing on the battery of a device and does not work indoors (for example, shopping malls). By scanning and collecting unique identifiers (in this case an Android ID) and the signal strength of Wi-Fi base stations near the device, Google can precisely calculate a consumer's location wherever they move in the world.

<sup>10</sup> Barometric pressure readings inform the altitude of the device and Wi-Fi scans inform the location reading, 38.877215, -76.9975140.



# HOW MUCH OF YOUR DATA DOES GOOGLE REALLY SHARE WITH YOU?

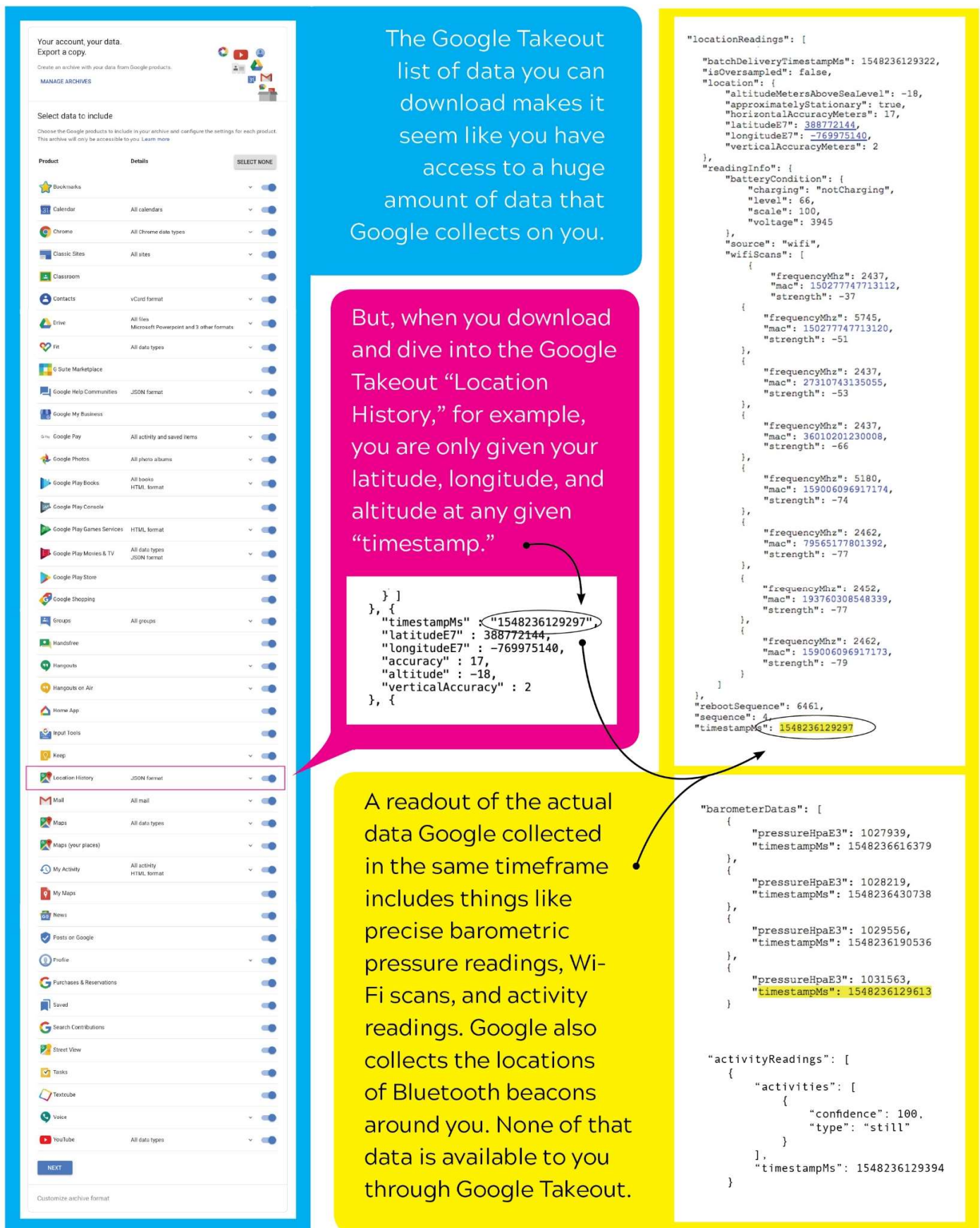
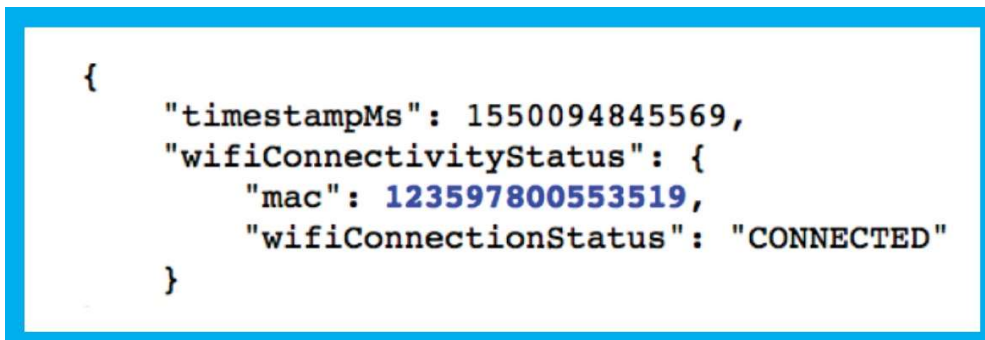


Figure 3: Google Takeout Data vs Data Transmitted to Google

Creating an up-to-date map of Wi-Fi base stations globally sounds daunting, but with more than 2 billion<sup>11</sup> active global Android users, Google can maintain a detailed database of access points updated constantly by the movements of unwitting consumers. Google's Bluetooth beacon database works in the same manner. And to ensure devices are located on the correct floor of a multi-story mall, Google uses the barometer data from Android devices to determine consumers' altitude. Clearly this data is valuable for Google, and it is collected directly from consumers' Android smartphones – however this data is missing from the Google Takeout documents.

Data about a consumer's movement and pattern of life allows Google to infer sensitive and unique information about consumers. Figure 4 is an example of a small amount of data collected by Google that initially seems benign (a record listing the Wi-Fi base station an Android device is connected to, along with a timestamp). Yet, if a consumer connects to the same Wi-Fi access point at 9 AM Monday-Friday, the Wi-Fi base station likely represents the consumer's place of work. Similarly, if a consumer connects to the same Wi-Fi base station every day at 7 PM and stays connected through the evening, the Wi-Fi base station is likely in located in the consumer's home.



```
{
  "timestampMs": 1550094845569,
  "wifiConnectivityStatus": {
    "mac": 123597800553519,
    "wifiConnectionStatus": "CONNECTED"
  }
}
```

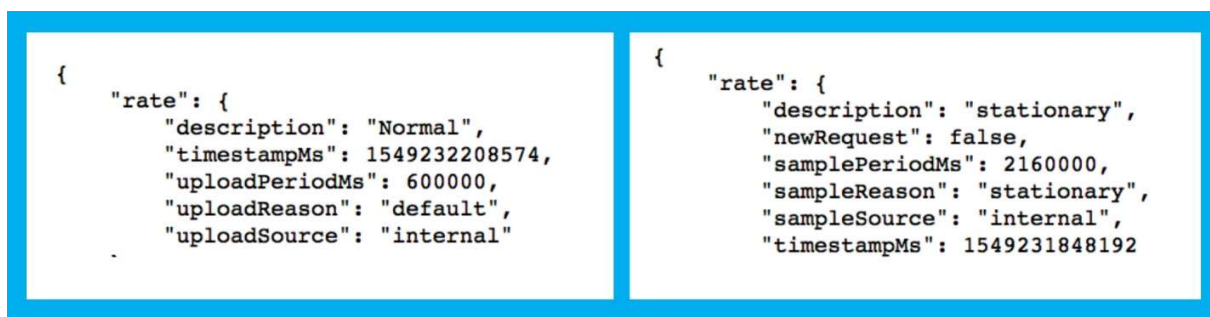
Figure 4: Andrea Tester's Android Device reporting Wi-Fi connection to Google

Google also records when the data collection rate on an Android device changes – an indication when a consumer is using or moving with the device. Figure 5 highlights two types of rate change records – an average or “Normal” rate (left), and a “stationary” rate (right). Just as with Wi-Fi base stations, Google can infer useful information from this seemingly benign data collection. If an Android smartphone phone is set for a normal rate of data collection until 10 PM every day, but then switches to a stationary rate of data collection until 5 AM, the consumer is likely asleep between these hours. When combined with data on Wi-Fi base stations (Figure 4), patterns of life can be readily inferred. However, Google does not provide the data it collects about connections to Wi-Fi base stations or changes in data collection rate to a consumer via its “Takeout” service.

The fact is that notwithstanding Google “takeout,” the information Google retains for itself is redundant such that it is as valuable for Google in targeting and tracking consumers for ads.

---

<sup>11</sup> <https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users>



Figures 5: Andrea Tester's Android Device reporting rate of data collection to Google

## In or Out - Google Collects and Uses Data at All Times

According to Google's privacy policy, "you can use many Google services when you're signed out or without creating an account at all."<sup>12</sup> Importantly, Google collects data on consumers even if the consumer does not have an account or is signed out:

*when you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using.*<sup>13</sup>

If a consumer with a Google Account signs out of Google services or attempts to use a feature of a Google Chrome web browser known as "Incognito Mode" (a supposedly privacy protective browsing mode Google markets), Google still tracks the consumer. In a letter to the United States House of Representatives Judiciary Committee Google CEO Sundar Pichai explains: "When a user conducts a search on Google in Chrome Incognito and signed-out modes, we set a cookie to correlate searches conducted in the same Incognito window during the same browsing session."<sup>14</sup> Pichai continues, "We will, however, use certain factors" ... "such as the browser type, language, time of search, location (or an estimation of location), and prior browser session searches, to improve Search ranking relevance for the user's query."<sup>15</sup> Google is still tracking the consumer via unique identifiers as outlined in their Privacy Policy, but never makes this data available to the consumer using Takeout.

## How Google Collects and Uses Data on Consumers without a Google Account

Mr. Pichai's explanation of how Google tracks consumers signed out of their Accounts or in incognito mode also provides insight into how Google tracks consumers who may not have a Google Account at all. Google still tracks these consumers when they interact with Google Services that do not require an account, such as Search or YouTube.

<sup>12</sup> <https://policies.google.com/privacy?hl=en#infocollect>

<sup>13</sup> <https://policies.google.com/privacy?hl=en#infocollect>

<sup>14</sup> Google CEO Sundar Pichai's response to US House Judiciary Questions for the Record. Page 3, Question 5.

<sup>15</sup> Google CEO Sundar Pichai's response to US House Judiciary Questions for the Record. Page 3, Question 6.



Google profits from a number of services and products that are not directly consumer facing and do not require a Google Account to use all of which are governed by Google's Privacy Policy.<sup>16</sup> For example, by shopping on JcCrew.com<sup>17</sup> or reading the news at NewYorkPost.com,<sup>18</sup> a consumer's behavior is now – unknowingly – governed by the Google Privacy Policy as those websites use Google Analytics. It is difficult, if not impossible, to use the internet without encountering Google Analytics as approximately 75% of the top 100,000 websites on the internet use Google Analytics.<sup>19</sup> In other words, consumers merely visiting websites on the internet have a 75% chance of being captured by Google's privacy (data collection) policy even if they have no other direct link to Google. Per its 2016 change in privacy policy, Google can then combine all of the data from its analytic properties with data generated by consumers using Google services to create a super-profile.<sup>20</sup>

Google explains to advertisers how this process occurs on its “demographic targeting” help page for ads:

*“For people who aren't signed in to their Google Account, we sometimes estimate their demographic information based on their activity from Google properties or the Display Network. For example, when people browse YouTube or sites on the Display Network, Google may store an identifier in their web browser, using a “cookie.” That browser may be associated with certain demographic categories, based on sites that were visited.”<sup>21</sup>*

Google tracks a consumer across sessions and stores the data they generate. For example, one of the features for Google Developers is a function called PlaceIDs.<sup>22</sup> (Figure 6) Consumers using Google Maps see different places populating the map, depending on the demographic data Google has collected about them. Google plainly explains to developers how invasive and profound Google's data collection is by remarkably stating on its Maps API documentation:

*“Every visitor to your site sees a Google Map tailored just for them”<sup>23</sup>*

Regardless of a consumer's Google account status or Location History setting, Google's algorithms determine which places to show each consumer based on a super-profile informed by the data Google collects. For example, if a signed-out user opens Google Maps and searches for Breckenridge, Vail and finally Tahoe, the user is likely to see a specific ski resort populate the map.

---

<sup>16</sup> Google's CEO Sundar Pichai's testimony to the U.S. House Judiciary Committee <https://www.c-span.org/video/?455607-1/google-ceo-sundar-pichai-testifies-data-privacy-bias-concerns&start=11932> (3:18:52)

<sup>17</sup> [https://www.jcrew.com/help/cookie\\_policy.jsp](https://www.jcrew.com/help/cookie_policy.jsp)

<sup>18</sup> <https://nypost.com/privacy/>

<sup>19</sup> <https://trends.builtwith.com/analytics/Google-Analytics>

<sup>20</sup> [https://www.google.com/intl/en\\_US/policies/privacy/archive/20160325-20160628/](https://www.google.com/intl/en_US/policies/privacy/archive/20160325-20160628/)

<sup>21</sup> <https://support.google.com/google-ads/answer/2580383?co=ADWORDS.IsAWNCustomer%3Dfalse&hl=en>

<sup>22</sup> <https://developers.google.com/places/place-id>

<sup>23</sup> <https://developers.google.com/maps/documentation/embed/guide>

This data is linkable to an individual via “unique identifiers” such as an Advertising ID or an IMEI<sup>24</sup> or the cookies described by Google above. This data can also be tied to the consumer’s location at the time of the search via their IP Address.<sup>25</sup>

In addition to being linked to a consumer through various unique identifiers, highly specific location data is unique to an individual over time. Google affirms this conclusion by offering advertisers the ability to serve highly targeted digital ads based on consumers’ location, regardless of those consumers’ Google account status.

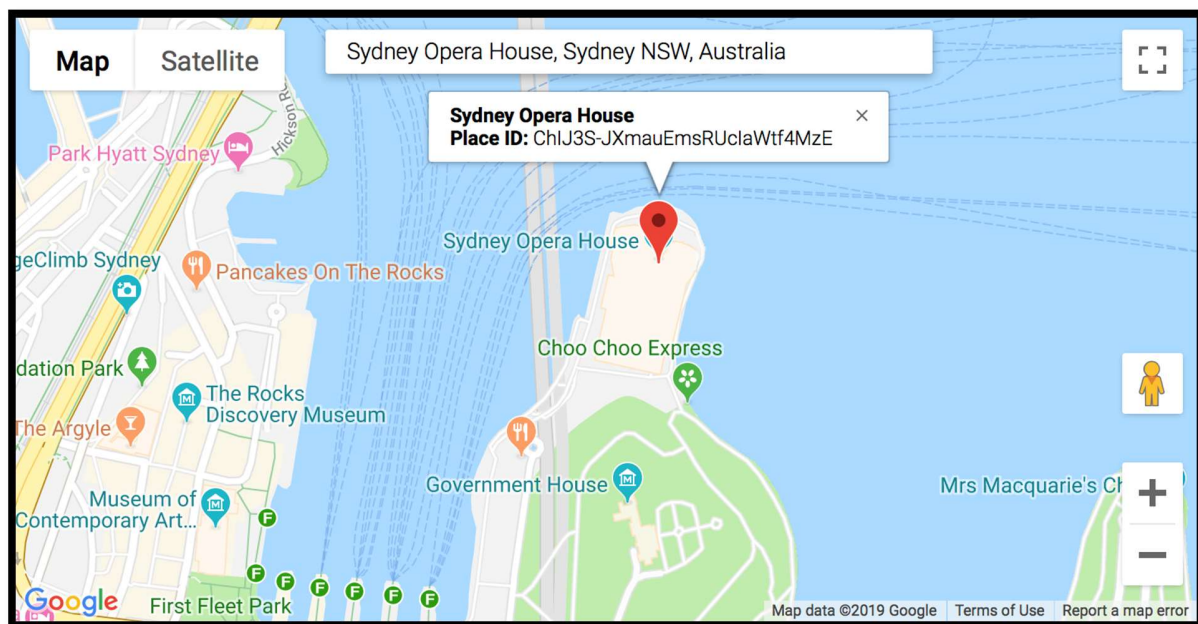


Figure 6: Google PlaceID for Sydney Opera House

## Data Google Collects about the World (via Consumers)

When a mobile Android device sends Google a consumer’s location, Google is able to maintain a self-updating and highly accurate map of devices moving throughout the world which can locate consumers in relation to various PlaceIDs on a map. Google claims to tell with 99% accuracy if, after seeing a digital advertisement for a store, a consumer enters the physical store location.<sup>26</sup> They can make this claim because Google has a detailed map of consumers’ movements, data on the dimensions of millions of retail locations,<sup>27</sup> and a database of PlaceIDs.

Evidence of Google’s constant location tracking are apparent in some of its consumer-facing products, such as Google reviews. (Figure 7) For example, the Google reviews of Sydney Opera

<sup>24</sup> <https://policies.google.com/privacy?hl=en#footnote-unique-id>

<sup>25</sup> <https://support.google.com/google-ads/answer/2453995?hl=en>

<sup>26</sup> <https://static.googleusercontent.com/media/www.google.com/en/us/adwords/start/marketing-goals/pdf/white-paper-bridging-the-customer-journey.pdf>

<sup>27</sup> <https://adwords.googleblog.com/2016/09/New-Digital-Innovations-to-Close-the-Loop-for-Advertisers.html>

House indicate the busiest times to visit are Friday and Saturday nights between 7 and 9 PM; this data is based off of visits to the location tracked surreptitiously on a consumer's smart phone, aggregated with the history of all consumers who have visited this location. Because Google has the world's most extensive database of places corresponding with specific locations, Google can link information about multiple devices at one location to assess busiest or most popular times for a given place.

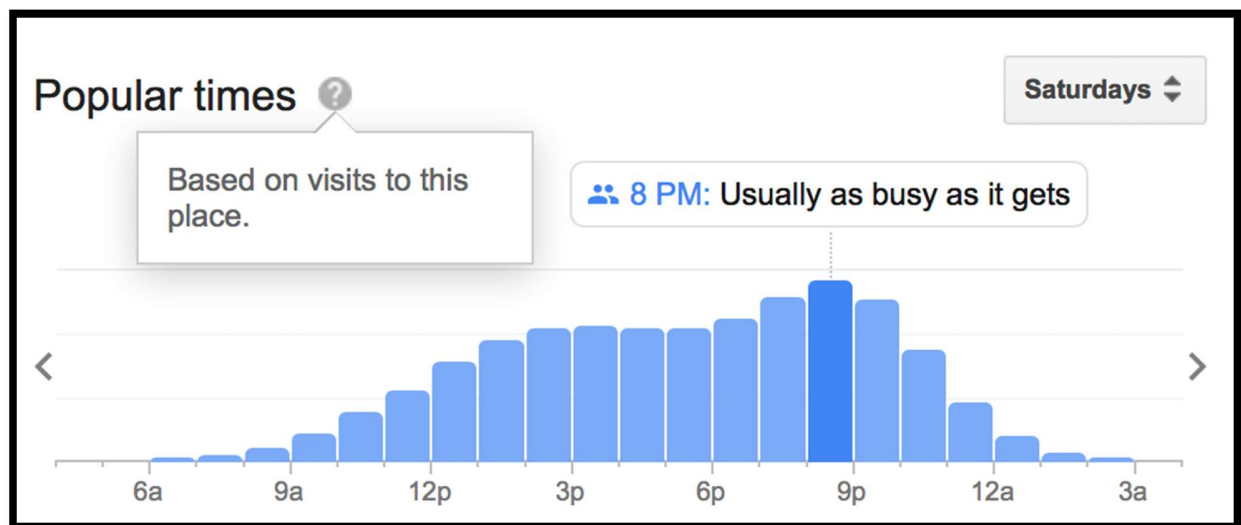


Figure 7: Google Reviews of Sydney Opera House

### Google Promotes its Consumer Location Tracking Capabilities to Advertisers

Despite public claims that Google “builds privacy that works for everyone,”<sup>28</sup> Google’s business model works to provide *everything but privacy* for the consumer. Google generates the majority of its revenue through advertising, powered by its ability to generate and combine large amounts of specific consumer data about consumer behavior on the internet with real time consumer activity and location data from mobile phones, as well as a myriad of other surreptitious collection points, such as internet cookies and application metadata. Google uses the location data it collects from mobile devices over time to establish patterns of life for consumers and acknowledges tracking both signed in and signed out consumers to infer interest in a location and inform a profile for the purposes of selling ads.

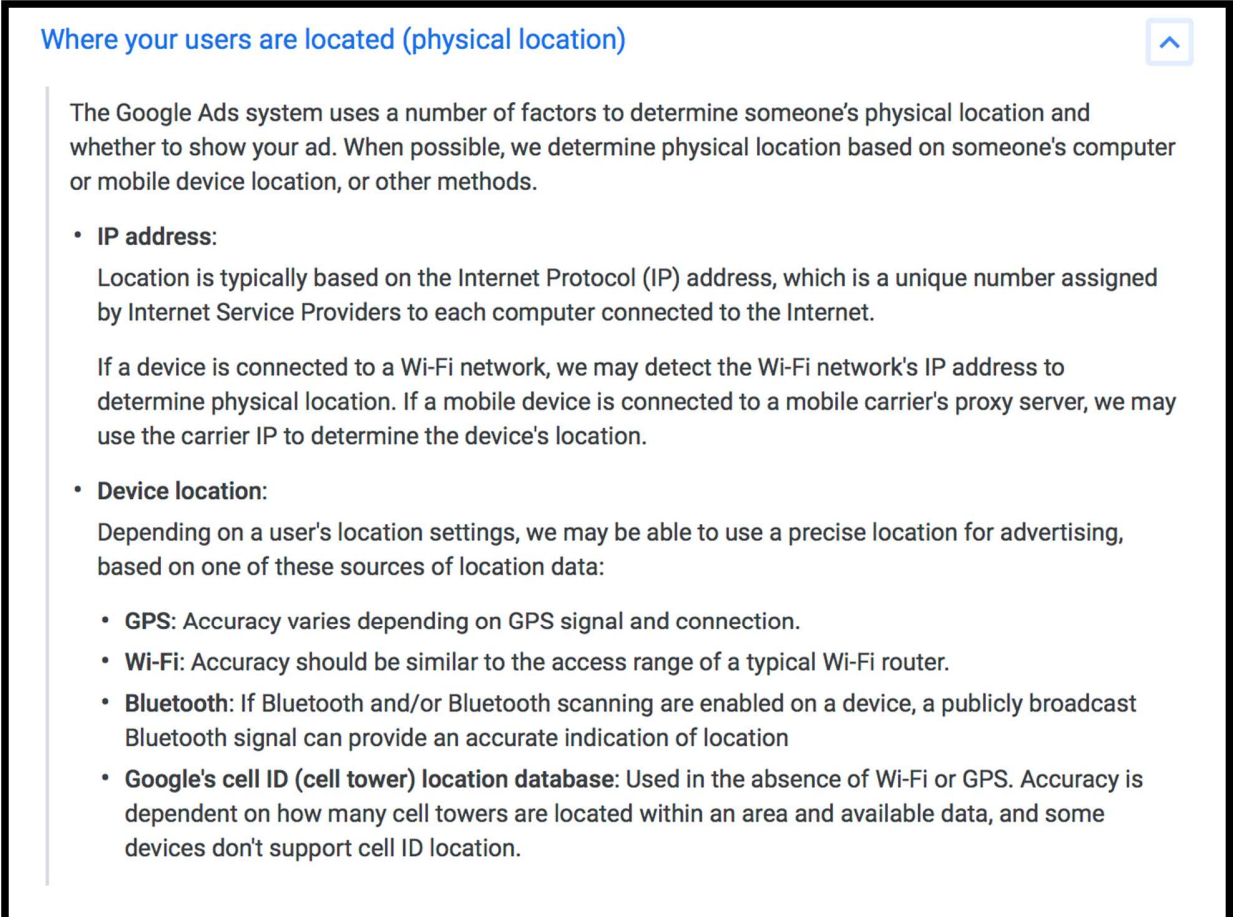
Google promotes its capability to target advertisements to a specific location in the world via IP Address and device location.<sup>29</sup> (Figure 8) In order for Google to target advertisements by a user’s

<sup>28</sup> <https://safety.google/privacy/>

<sup>29</sup> <https://support.google.com/google-ads/answer/2453995?hl=en>

IP Address or the location of a device, it is reasonable to conclude Google must collect and tie this data back to individual consumers, feeding the result into digital advertising profiles.

Even though consumers are told they are “in control” of how Google collects and uses their data,<sup>30</sup> there is no way to disable location tracking via IP Address. Despite its relevance to consumers and advertisers, historical IP Address-based location information is not available to consumers via the Google Takeout service. Similarly, the catalogue of GPS and Cell Tower location data, Wi-Fi base station and Bluetooth beacon scans Google uses to locate consumers is not available via Takeout. And of course, none of this information is available to consumers who do not have a Google Account, but are uniquely identified and tracked by Google.



The screenshot shows a help article titled "Where your users are located (physical location)" with a blue header and a small icon in the top right corner. The main text explains that the Google Ads system uses various factors to determine physical location. It lists two main categories: "IP address" and "Device location". Under "IP address", it states that location is typically based on the Internet Protocol (IP) address and provides details about Wi-Fi networks and mobile carrier proxy servers. Under "Device location", it lists four sources: GPS, Wi-Fi, Bluetooth, and Google's cell ID (cell tower) location database, each with a brief description of how they determine location.

**Where your users are located (physical location)**

The Google Ads system uses a number of factors to determine someone's physical location and whether to show your ad. When possible, we determine physical location based on someone's computer or mobile device location, or other methods.

- **IP address:**  
Location is typically based on the Internet Protocol (IP) address, which is a unique number assigned by Internet Service Providers to each computer connected to the Internet.  
  
If a device is connected to a Wi-Fi network, we may detect the Wi-Fi network's IP address to determine physical location. If a mobile device is connected to a mobile carrier's proxy server, we may use the carrier IP to determine the device's location.
- **Device location:**  
Depending on a user's location settings, we may be able to use a precise location for advertising, based on one of these sources of location data:
  - **GPS:** Accuracy varies depending on GPS signal and connection.
  - **Wi-Fi:** Accuracy should be similar to the access range of a typical Wi-Fi router.
  - **Bluetooth:** If Bluetooth and/or Bluetooth scanning are enabled on a device, a publicly broadcast Bluetooth signal can provide an accurate indication of location
  - **Google's cell ID (cell tower) location database:** Used in the absence of Wi-Fi or GPS. Accuracy is dependent on how many cell towers are located within an area and available data, and some devices don't support cell ID location.

Figure 8: Google Ads Help Explanation Targeted Ads by Geolocation

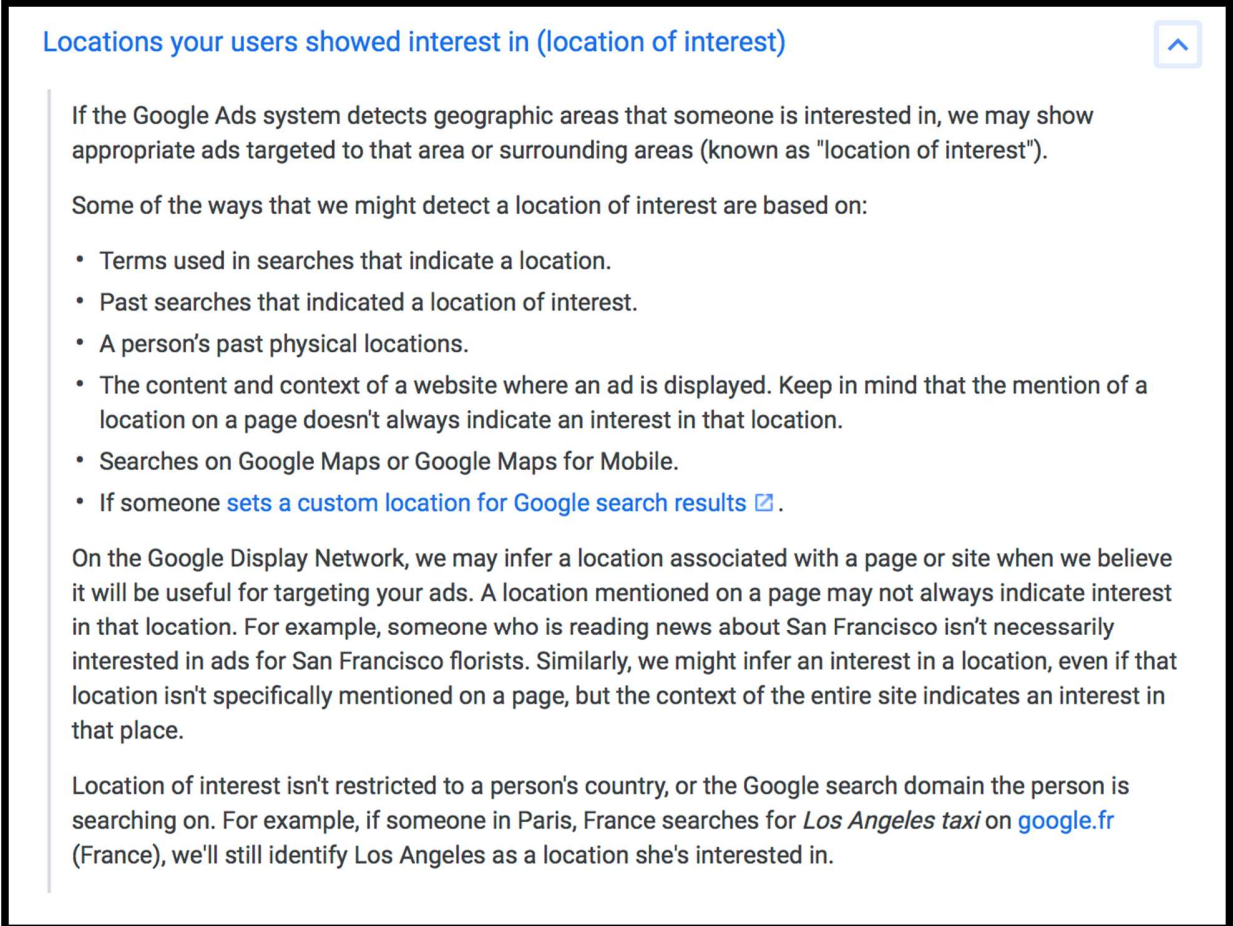
Google also allows advertisers to target consumers based on their interest in a location, and highlights the value of tracking consumer location over time. (Figure 9).<sup>31</sup> Among other factors,

<sup>30</sup> <https://safety.google/privacy/privacy-controls/>

<sup>31</sup> <https://support.google.com/google-ads/answer/2453995?hl=en>



Google infers a consumer's interest in a location based on their physical history at a particular location as well as searches on Google Maps.



The screenshot shows a help article titled "Locations your users showed interest in (location of interest)". The text explains that Google Ads uses geographic data to show targeted ads. It lists several ways Google detects location interest: terms in searches, past searches, past physical locations, website content and context, Google Maps searches, and custom locations set by users. It also notes that location interest is not limited to a person's country or the search domain.

**Locations your users showed interest in (location of interest)**

If the Google Ads system detects geographic areas that someone is interested in, we may show appropriate ads targeted to that area or surrounding areas (known as "location of interest").

Some of the ways that we might detect a location of interest are based on:

- Terms used in searches that indicate a location.
- Past searches that indicated a location of interest.
- A person's past physical locations.
- The content and context of a website where an ad is displayed. Keep in mind that the mention of a location on a page doesn't always indicate an interest in that location.
- Searches on Google Maps or Google Maps for Mobile.
- If someone [sets a custom location for Google search results](#).

On the Google Display Network, we may infer a location associated with a page or site when we believe it will be useful for targeting your ads. A location mentioned on a page may not always indicate interest in that location. For example, someone who is reading news about San Francisco isn't necessarily interested in ads for San Francisco florists. Similarly, we might infer an interest in a location, even if that location isn't specifically mentioned on a page, but the context of the entire site indicates an interest in that place.

Location of interest isn't restricted to a person's country, or the Google search domain the person is searching on. For example, if someone in Paris, France searches for *Los Angeles taxi* on [google.fr](#) (France), we'll still identify Los Angeles as a location she's interested in.

Figure 9: Google Ads Help Explanation Targeted Ads by Geolocation

## From Data to Dollars

A consumer's pattern of life – the daily rhythm of the people and places individuals spend time in the real world – combined with online web browsing, search history and a myriad of other data points creates an intimate dossier of a consumer's lifestyle. Google uses this data to develop and continuously update its super-profile on consumers. Combining multiple sources of user data across its products, services devices and accounts, the pool of data is used to power Google's digital advertising, responsible for 86% of Google's revenue.<sup>32</sup>

Through its various digital services, Google is able to track consumers across the internet. These services include what a consumer can directly link to their Google Account, (Search, YouTube, Gmail, Hangouts, etc.) as well as various AdTech and Analytic Products where a consumer may

<sup>32</sup> [https://abc.xyz/investor/static/pdf/20171231\\_alphabet\\_10K.pdf?cache=7ac82f7](https://abc.xyz/investor/static/pdf/20171231_alphabet_10K.pdf?cache=7ac82f7)

not have a direct relationship (Google Ads, DoubleClick, Google Analytics, etc). Google does not claim to target individual consumers with specific ads, rather, Google works at a larger scale - targeting *all* consumers based off of their individual demographics, location, and intent. Within Google's ad products, there are multiple ways to target specific advertising "audiences." According to Google, audiences are "groups of people with specific interests, intents, and demographics, *as estimated by Google*" (emphasis added).<sup>33</sup> Most broadly, an advertiser can target an ad campaign based on various demographic data points.<sup>34</sup> In a letter to the US Senate, Google explains how it infers demographic data based on a consumer's location for the purposes of advertising.<sup>35</sup>

Audience specific targeting allows advertisers to reach consumers based on their individual interests, a feature Google calls "affinity audiences"<sup>36</sup> (Figure 10), as well as their intent, called "in-market audiences".<sup>37</sup> (Figure 11) Google makes assessments of a consumer's affinity and / or intent based off of the data collected on consumers via their interaction with Google's Services (such as Android or websites that use Google's advertising or analytic products). To further refine an audience, an advertiser can target websites related to varying subjects, called "targeted topics".<sup>38</sup> (Figure 12)

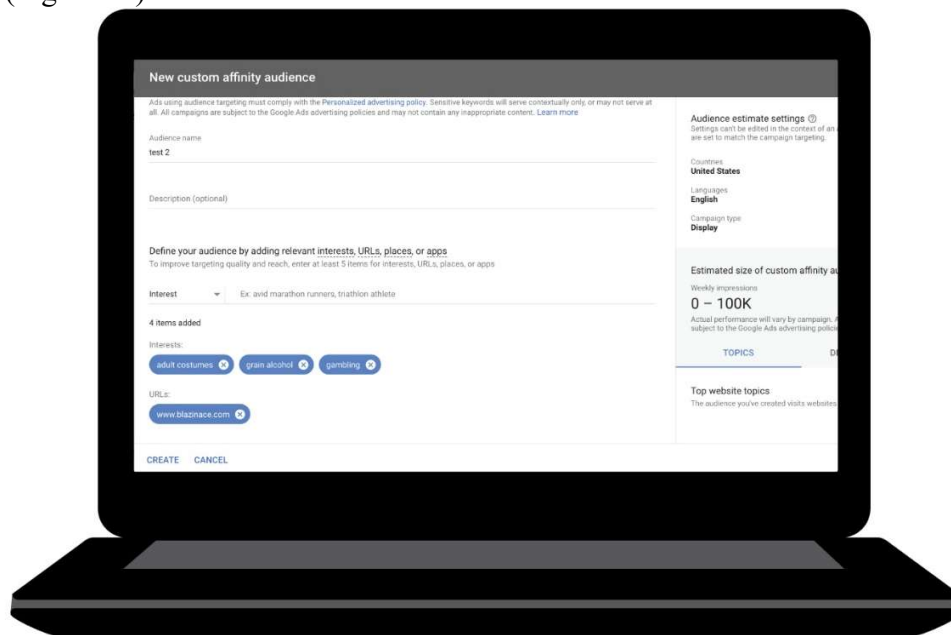


Figure 10: Sample Affinity Audiences on Google Ads Platform

<sup>33</sup> <https://support.google.com/google-ads/answer/2497941?hl=en>

<sup>34</sup> <https://support.google.com/google-ads/answer/2580383?co=ADWORDS.IsAWNCustomer%3Dfalse&hl=en&oco=0>

<sup>35</sup> Letter from Google to US Senate (Page 5, Paragraph 3)  
<https://www.blumenthal.senate.gov/imo/media/doc/05.11.2018%20-%20FTC%20-%20Google%20Location%20History.pdf>

<sup>36</sup> [https://developers.google.com/adwords/api/docs/appendix/affinity\\_categories.csv](https://developers.google.com/adwords/api/docs/appendix/affinity_categories.csv)

<sup>37</sup> [https://developers.google.com/adwords/api/docs/appendix/in-market\\_categories.csv](https://developers.google.com/adwords/api/docs/appendix/in-market_categories.csv)

<sup>38</sup> <https://support.google.com/google-ads/answer/2497832?hl=en>

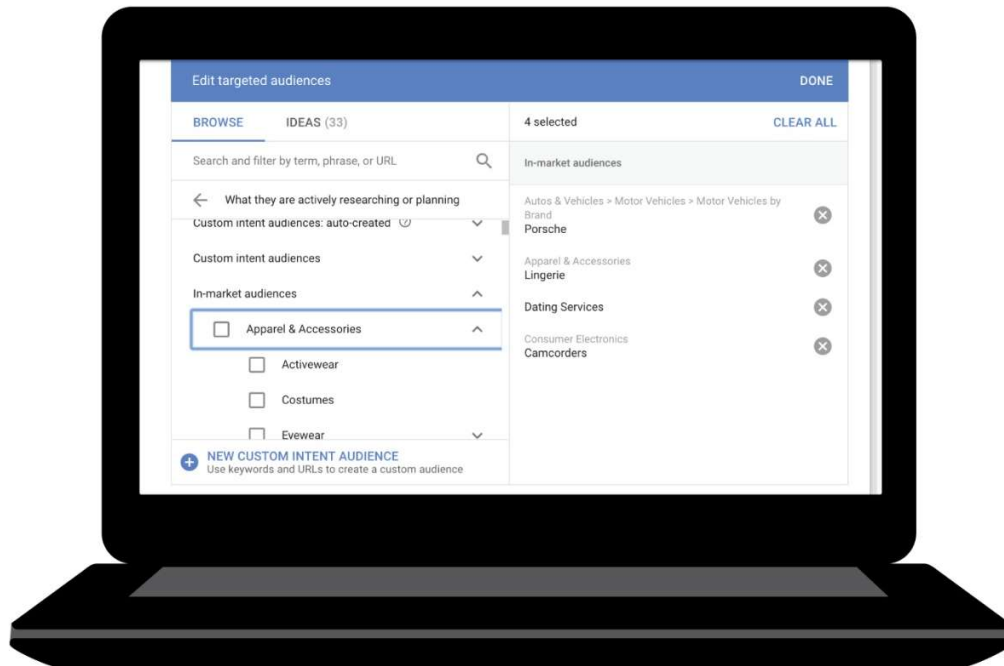


Figure 11: Sample In-Market Audiences on Google Ads Platform

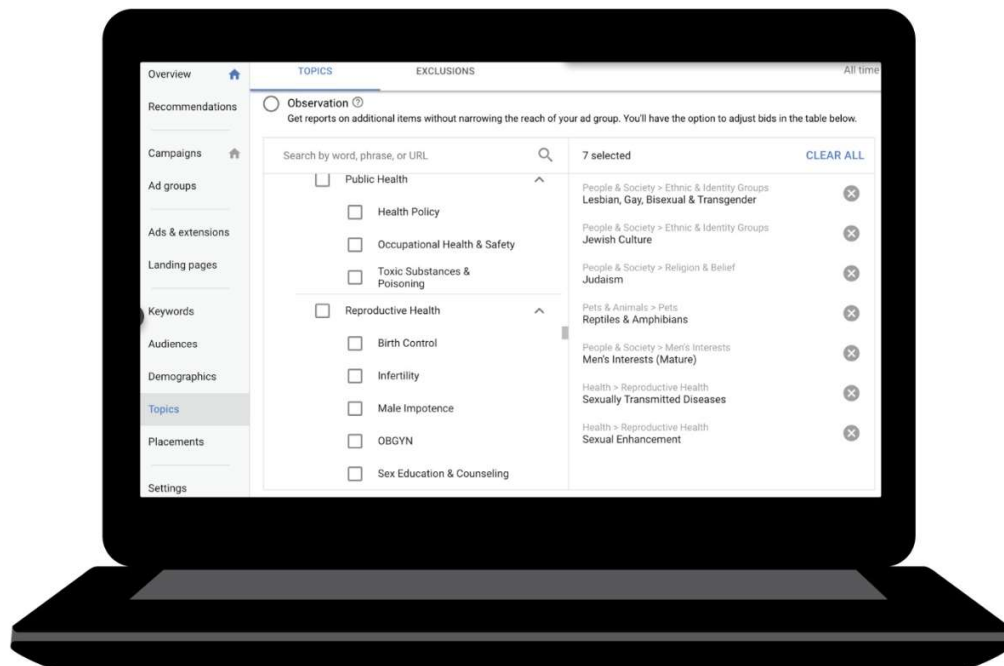


Figure 12: Sample Targeted Topics of Google Ads Platform

Advertisers have the ability to combine data sets across demographic, affinity, and intent audiences. For instance, an advertiser could target a 40-year-old married male with children that makes \$50k a year whose interests are:

- “adult costumes”
- “grain alcohol”
- “gambling”

The same advertiser could then combine this profile with an intent such as:

- “gentlemen’s club”
- “infectious diseases”
- “male enhancement”

To build upon the above example, an advertiser could combine the outlined profile of an individual with topics that same consumer might interact with on the internet. Google’s ad product provides options for topics such as:

- “divorce & separation”
- “depression”
- “male impotence”

By targeting against websites with specific topics, an advertiser can also indirectly target an audience. Any consumer’s interaction with a “topic” would also feed their “audience” profile. If the hypothetical consumer described above interacts with advertisements Google served against their interests, intent, and online activity, the interaction itself will add to the profile of this consumer, data that Google can use to improve targeting for advertisers.

Once a consumer interacts with an advertisement, the advertiser can add that individual to a “remarketing list,” allowing direct targeting of the individual in subsequent ad campaigns. Google also offers the ability to target “similar audiences” “to people who share characteristics with people on your existing remarketing lists”.<sup>39</sup> Google’s data collection can reveal individuals who just *may* be interested in a product or service simply because that consumer is *similar* to another consumer who has demonstrated interest in a product.

## Summary

Google’s business is designed to collect as much data as possible about as many consumers as possible. Yet only a small amount of the data Google collects is made available to Google account holders even though Google claims to provide an exhaustive list of the data collected. In reality, Google collects and stores significantly more data about each consumer, if they have a Google account or not, and ties this data to unique identifiers which enable it to link information back to an individual. The information that Google does not reveal to a consumer is that consumer’s shadow profile. As a result consumers do not fully understand all of the data Google holds, which Google uses to target consumers at any moment across various products and services and is continuously updated as consumers navigate the internet and the real world.

---

<sup>39</sup> <https://support.google.com/google-ads/answer/7139569?co=ADWORDS.IsAWNCustomer%3Dtrue&hl=en&oco=0>



## *Attachment B: Google Stealthily Enables 'Super-Profiles'*

### *Company Combines Personal Information with of Data from Third-Party Sites and Apps without Opt-In Consent*

#### **Executive Summary**

On June 28, 2016, Google quietly changed its policies and settings, telling its users it was offering “new features” that would grant them greater control over their own information. The change attracted little attention; many users simply agreed and moved on.

But this change had a profound effect on the amount of information that Google holds on virtually everyone who comes into contact with the internet, and made it nearly impossible for users to escape the company’s tracking of their activities.

The change allowed Google, for the first time, to combine data gathered from cookies that track browsing behavior on nearly 80% of websites<sup>1</sup> with the trove of personal information it holds from its own user accounts. Previously, Google had maintained two separate profiles on each user: one combining data from its own services, such as Gmail, Google Search, YouTube, Android devices, and other proprietary services; the other that tracked user activity on sites that use Doubleclick Advertising and Google Analytics cookies.

The 2016 policy change allowed Google to join these two vast repositories of data into “super-profiles” of internet users, realizing the fears advanced by privacy advocates when Google acquired Doubleclick in 2007.<sup>2</sup> In fact, those concerns have been eclipsed by Google's current policy, which not only allows Google to include data from Doubleclick cookies that track users’ browsing across the web, but also information from *any* app or site that uses Google Services, including Google Analytics, embedded YouTube video, and potentially third-party Android apps that use Google’s programming interfaces.

In other words, Google’s stealth advertising profiles now include data from any website that uses Google Analytics,<sup>3</sup> hosts YouTube videos, displays ads served by Doubleclick or AdSense — the overwhelming majority of sites in use in the world today. And it can add to that data it gets from a user’s Android phone even when they are not actively using the web, including their location, activity, even local weather conditions.

The move represented a step change in the amount of information that Google has on file about billions of people in order to sell to advertisers. It also made it virtually impossible for Google users to avoid being tracked by Google: The company claims that over 90% of Internet users worldwide

---

<sup>1</sup> A 2015 survey of the top one million web domains found Google trackers on nearly eight out of ten sites: <http://ijoc.org/index.php/ijoc/article/view/3646/1503>

<sup>2</sup> Statement of Marc Rotenberg, Executive Director Electronic Privacy Information Center; Committee on Senate Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights; September 27, 2007

<sup>3</sup> Estimated at 30-50 million web pages: <http://marketingland.com/as-google-analytics-turns-10-we-ask-how-many-websites-use-it-151892>

come into contact with its Google Display Network.<sup>4</sup> And it made it harder for other advertising providers to compete, further entrenching Google's monopoly.

The 2016 change represented the culmination of Google's decade-long effort to build increasingly detailed profiles of people's lives. Since it began providing "context-based" searches based on the contents of users' emails and search requests, Google has built its business around tailoring ads to user information.

In 2009, following its controversial acquisition of Doubleclick, Google introduced "interest-based" ads that profiled users according to their browsing activity. At the time, Google kept those browsing profiles separate from user account data, as a concession to privacy advocates. The company amended its privacy policy in 2012 to state that it would not combine data from Doubleclick with users' accounts without their opt-in consent.<sup>5</sup>

The 2016 policy change reneged on this commitment and unified Google's discrete pools of user data, granting the company greater insight into users' behaviors and preferences without adequately explaining the consequences of that data collection to users. The change may have violated the terms of a 2011 consent decree by failing to clearly and prominently disclose the sources of third-party data sharing and by moving from an 'opt-in' to an 'opt-out' consent model.

## Key Findings

- One June 28, 2016, Google changed its privacy policy to allow it to combine information gathered from third party sites and apps with personal information that users share with Google.
- Google removed a clause requiring it to obtain opt-in consent before combining data from its advertising network with personal information. The default is now opt-out consent.
- Current policy allows Google to combine personal information with data gathered from sites or apps that use *any* Google services, including Doubleclick, AdSense, Google Analytics, embedded YouTube video, and Android APIs managed through Google Play Services.
- Google does not state the full scope of data collection on users' ads settings pages or on its main privacy policy page. The company only offers a definition of its "partners" that collect user data in a pop-up footnote.
- By combining Doubleclick data with personal account information, Google is now able to create 'super-profiles' that capture nearly all of a user's web activity, realizing the fears that privacy advocates raised when Google acquired Doubleclick.
- Google may have violated a 2011 consent decree by failing to clearly and prominently disclose the sources of third-party data sharing and by moving from an opt-in to an opt-out consent model. Further information on the consent decree is set out in the attachment to this paper.
- Combining data gathered through its advertising network and other web services with account data allows Google to track users across devices. Tracking "cross-device conversions" has become a critical component of the company's advertising business.

---

<sup>4</sup> [https://support.google.com/adwords/answer/2404191?hl=en&ref\\_topic=3121944](https://support.google.com/adwords/answer/2404191?hl=en&ref_topic=3121944)

<sup>5</sup> [https://www.google.com/intl/en\\_US/policies/privacy/archive/20111020-20120301/](https://www.google.com/intl/en_US/policies/privacy/archive/20111020-20120301/)

## Privacy Policy Change and ‘Ads Personalization’

On June 28, 2016, Google quietly changed its policy governing the use of customer data.<sup>6</sup> It removed the restriction on combining user data gathered via its Doubleclick advertising service with information gleaned from users’ activity on Google products, and asserted its right to combine data from third party apps or sites with personal information associated with users’ accounts.

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. ~~We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.~~ Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

Changes to Google’s privacy policy, June 2016

All websites that display ads through Google contain the Doubleclick tracking cookie, a tiny text file that follows users across the internet.<sup>7</sup> When a user visits a site that serves ads using Google technology, the site places a cookie on her browser.<sup>8</sup> The cookie identifies the browser and keeps track of the sites that it visits, the ads that it sees, and how the user interacts with webpages.<sup>9</sup> The 2016 privacy policy change allowed Google to store this browsing data in signed-in users’ accounts, creating a persistent record of browsing data that can be triangulated with a user’s personal information.<sup>10</sup>

Now, when a user signs on to any Google service, such as Gmail, YouTube, or Search, Google associates the browsing history stored in the Doubleclick tracking cookie with her profile.<sup>11</sup> Once a user signs in to a google service, she remains signed in on that browser until she affirmatively signs out. As long as the user remains signed in, Google continues to collect browsing data in real time. When a signed-in user visits a site with Google tracking technology, it joins a user identifier with the site’s own traffic data.<sup>12</sup>

In 2018, Google made a play for even deeper insight into users’ browsing activity by automatically signing users into the Chrome browser when they signed into their Google accounts.<sup>13</sup> The move would allow Google to collect browsing data even from users who block Doubleclick cookies or otherwise attempt to opt-out of third party data collection.

---

<sup>6</sup> <https://www.google.com/intl/en/policies/privacy/archive/20160325-20160628/>

<sup>7</sup> <https://support.google.com/adsense/answer/48182>

<sup>8</sup> <https://support.google.com/adsense/answer/2839090?hl=en>

<sup>9</sup> <https://support.google.com/adsense/answer/2839090?hl=en>

<sup>10</sup> <https://support.google.com/adsense/answer/2839090>

<sup>11</sup> <https://support.google.com/adsense/answer/2839090?hl=en>

<sup>12</sup> <https://www.beanstalkim.com/blog/2017/04/update-remarketing-google-analytics/>

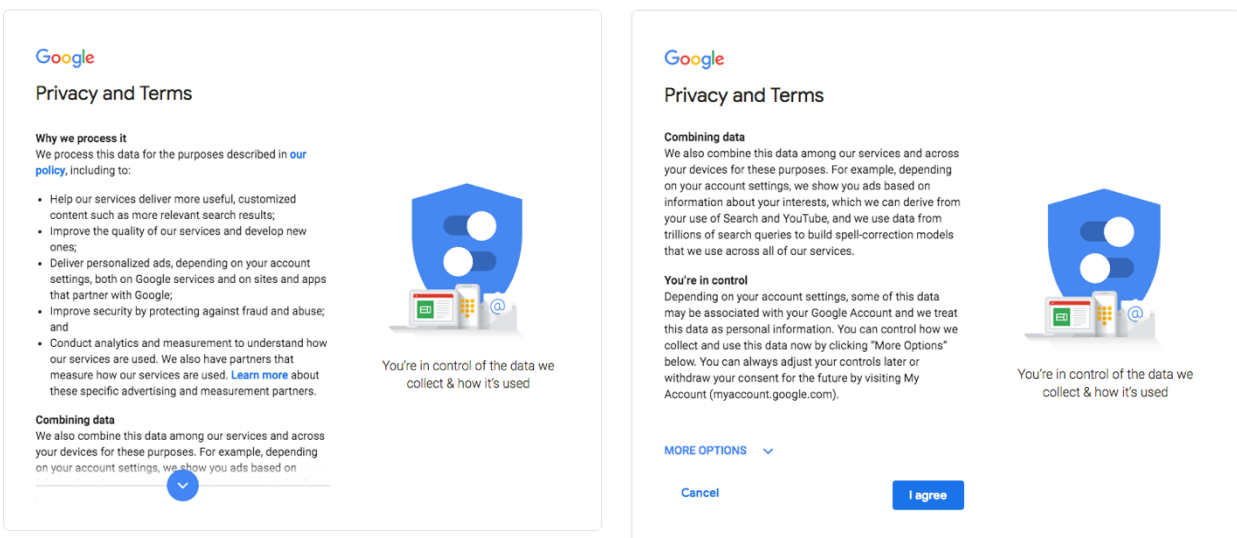
<sup>13</sup> <https://techcrunch.com/2018/09/24/security-experts-say-chrome-69s-forced-login-feature-violates-user-privacy/>

## Google Abandons its Opt-In Consent Model

Google's 2016 privacy policy removed any mention of obtaining users' opt-in consent for data consolidation. To this day, Google's privacy policy makes no mention of opt-in consent for data collection, and the company's ads settings page suggests that the company has moved to an opt-out privacy regime.<sup>14</sup>

Google accounts now default to gathering and combining user data from all Google services, advertisers, and third-party apps and sites. When the 2016 policy change was first introduced, Google required users opening new accounts to accept a notification explaining that Google collects and combines this information before proceeding with account creation. Until 2018, Google did not provide users with an option to opt out immediately upon creating a new account.

Following revisions to the company's privacy policy to comply with the European General Data Protection Regulation, Google began offering the option to opt out of data collection and combination upon creating a new account.<sup>15</sup> Users can only access this option by clicking a link for "more options" in a pop-up window detailing Google's data collection practices. Google does not otherwise prompt users to review their privacy settings upon account creation, and maximally-invasive data collection is turned on by default.



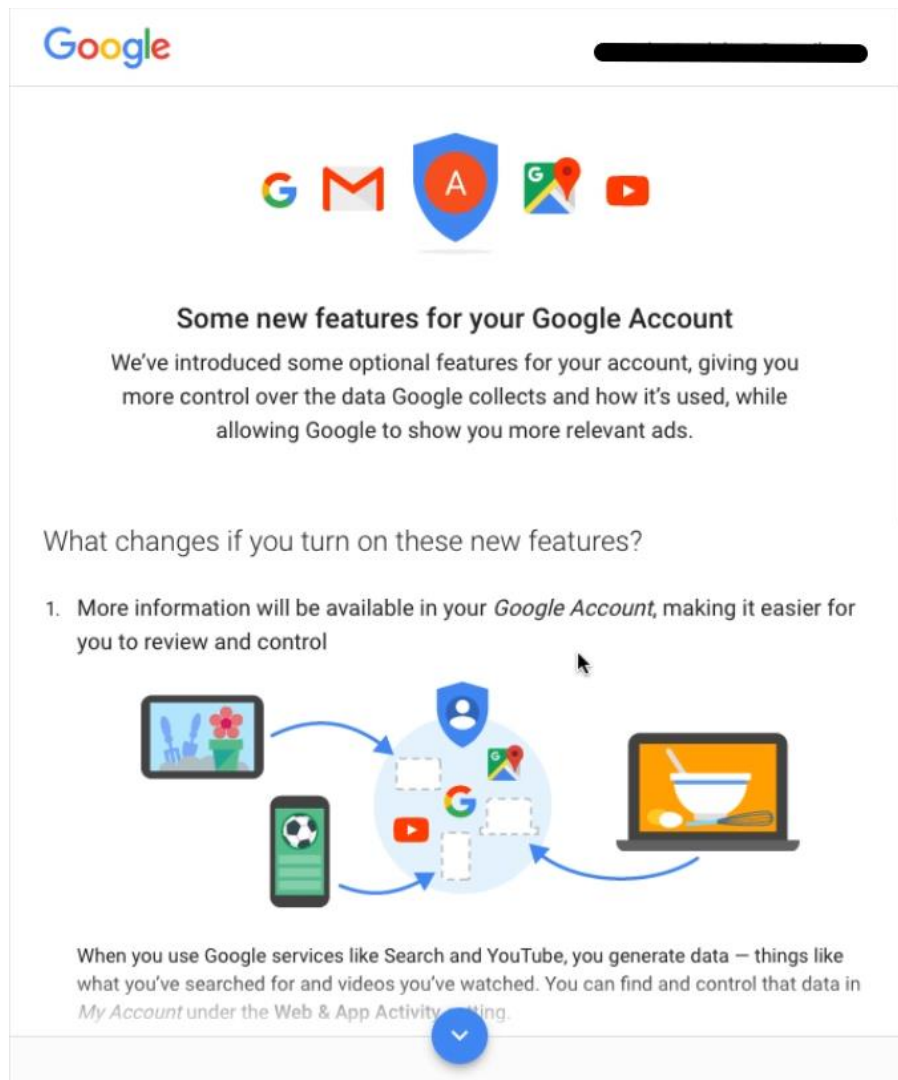
In order to create a new Google account, users must agree to a privacy policy that states that Google will collect data from third parties and combine it with their personal information.

<sup>14</sup> <https://policies.google.com/privacy>, <https://support.google.com/ads/answer/2662922?hl=en-GB>

<sup>15</sup> <https://accounts.google.com/signup/v2/webcreateaccount?continue=https%3A%2F%2Faccounts.google.com%2FManageAccount&flowName=GlifWebSignIn&flowEntry=SignUp>

Google also stretched the definition of opt-in consent for existing users. Existing users received a misleading notification in the Gmail web interface advertising “new features for your Google Account.” The notification obscured the fact that Google had changed its privacy policy and that these new features would dramatically expand the dossiers that the firm maintains on its users.

The notification does not make immediately clear how to opt out of the broader data collection. It ends with “Choose I AGREE to turn these features on or MORE OPTIONS for more choices.”



With this change, this setting may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.

2. Google will use this information to make ads across the web more relevant for you



In *My Account*, the **Ads Personalization** setting currently lets Google use data in your account to tailor ads that appear in Google products.

With this change, this setting will also let Google use data in your account to improve the relevance of ads on websites and apps that partner with Google.

These settings apply across all of your signed-in devices and across all Google services. You can change them any time in *My Account*. [Learn more](#) about these features, including how they affect shared devices.

#### What's still the same?

- Google does not sell your personal information to anyone
- You control the types of information we collect and use at *My Account* ([myaccount.google.com](https://myaccount.google.com))

**Choose I AGREE to turn these features on or MORE OPTIONS for more choices.**

[MORE OPTIONS](#)



**I AGREE**

Google required users to select one of these options to get to their mailboxes. Users who selected “I AGREE,” consented to combining tracking data from third party sites and apps with personal account data, without learning more about the scope of the data collection.

Users who selected “More Options” received yet another notification, presenting them with three choices: “No changes – continue to Gmail,”<sup>16</sup> “No changes – review key privacy settings more fully,” or “Yes, I’m in – turn on these new features.”

---

<sup>16</sup> Earlier iterations of this notification read, “No changes – continue on your way.”



### Choose what's right for you


Need more info first?  
[Learn more about these features](#)

☐ **No changes – continue to Gmail**  
We won't change anything and your Google experience, including the ads you see, will remain the same

☐ **No changes – review key privacy settings more fully**  
Take the *Privacy Checkup* to review key settings, including settings for ads

☐ **Yes, I'm in – turn on these new features**  
You can change your mind anytime at *My Account*

[BACK](#)



[DONE](#)

Users who clicked on “No changes – continue to Gmail” opted out of the new policy – but their underlying ads settings did not clearly indicate that combining third party data with personal information was turned off. Instead, a setting called “Ads based on your interests on sites beyond google.com” was set to neither on nor off, with a prompt that read, “please set your ads preference.”



# Control your Google ads

You can control the ads that are delivered to you based on anonymous information by editing these settings. These ads will more likely be useful and relevant to you and your Google services, such as search.

## New features that give you even more control

We've introduced some optional features for your Google Account that give you even more visibility and control of your data, while allowing Google to show you more relevant ads. More control of your data means even more control of the ads Google shows.

[LEARN MORE](#)



### Please set your ads preference

Ads based on your interests can be switched on or off.

Ads based on your interests on websites beyond google.com

OFF ☐ ON ☒

#### With Ads based on your interests ON

- You can mute some ads that you don't want to see
- You may see ads related to factors such as your interests and previous visits to other websites (remarketing)
- The ads may be based on anonymous demographic details such as age and gender
- The ads may be based on your general location (such as city or state) or the current page or app you are looking at

#### With Ads based on your interests OFF

- You will still see ads
- The ads will be less relevant to you
- You will be opted-out of interest based ads that are part of the Google Display Network and Google ads that are based on visits to advertiser websites (remarketing)
- The ads may be based on your general location (such as city or state) or the current page or app you are looking at

Google Search Ads based on your interests

☒ ON

#### With Ads based on your interests ON

- Ads will be more relevant by considering your prior searches and you may see fewer ads
- Ads you see are more likely to be about products and services you have previously searched for
- Ads may be more appropriate for your age and gender based on anonymous demographic details

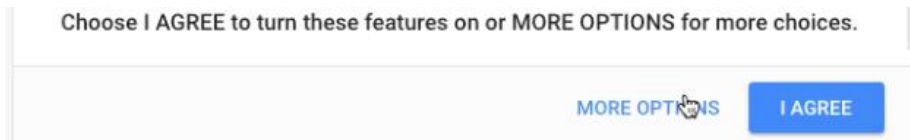
#### With Ads based on your interests OFF

- You will still see ads
- The ads will be less relevant to you
- An advertiser can't factor into their ads your previous visits to their website (search remarketing)

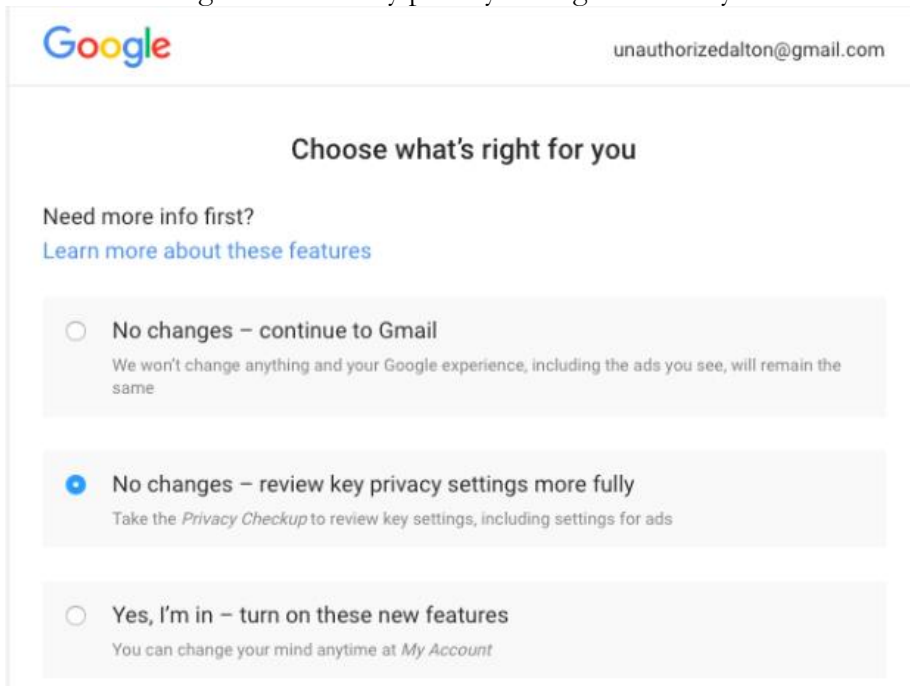
Users who selected “No changes – review key privacy settings more fully” were led through at least ten clicks before they reach their ads personalization page. At minimum, they had to:

1. Click “More options” on the initial “New features for your Google Account” notification

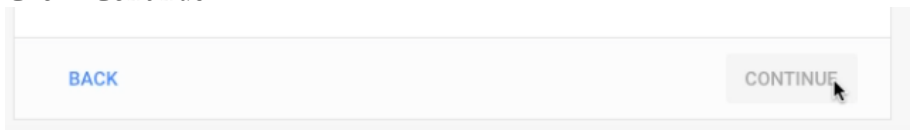




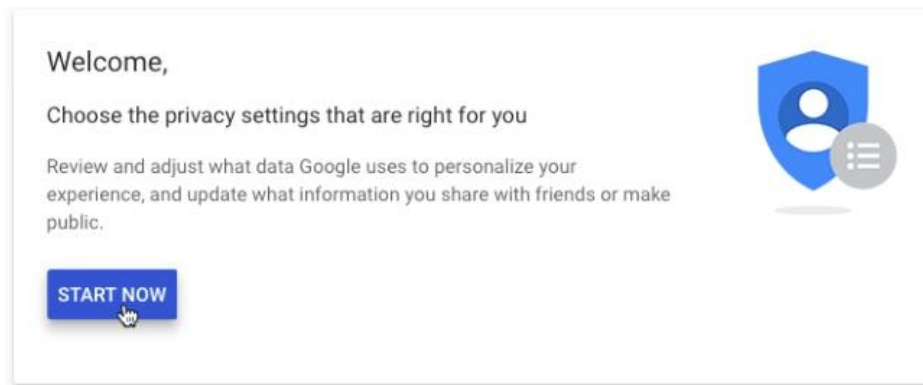
2. Click “No changes – review key privacy settings more fully”



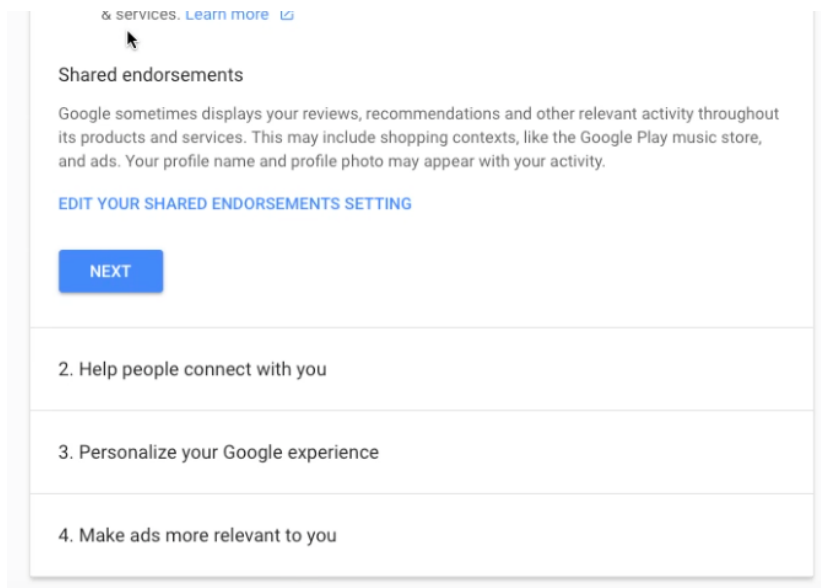
3. Click “Continue”



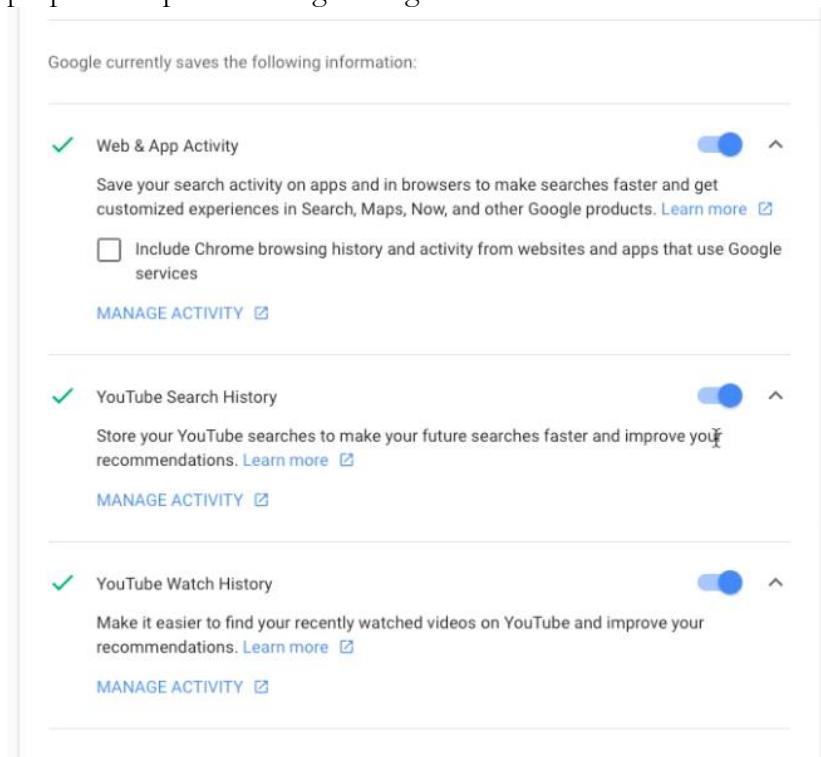
4. Click “Start Now”



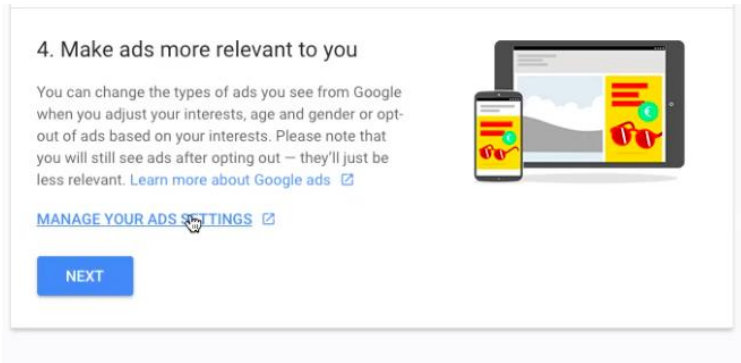
5. At minimum, click “Next” three times, once each on “Choose what Google+ profile information you share with others”, “Help people connect with you”, and “Personalize your Google experience.”



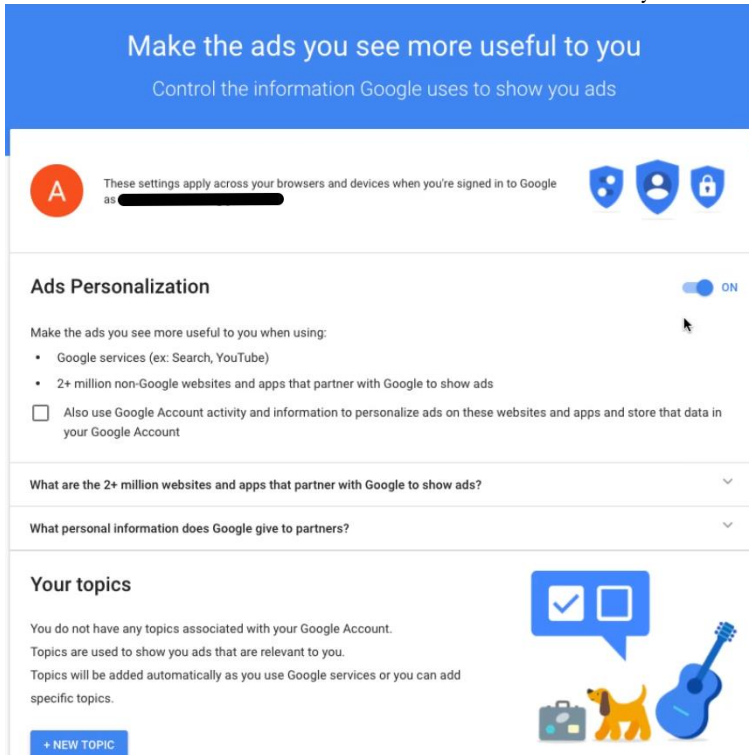
6. Google required an additional six clicks to opt out of the company's tracking of search and browsing activity on the web. Critically, this tracking is entirely separate from Google's ads settings – Google continues to track users who opted out of ads but not tracking for the purpose of "personalizing" Google's other services.



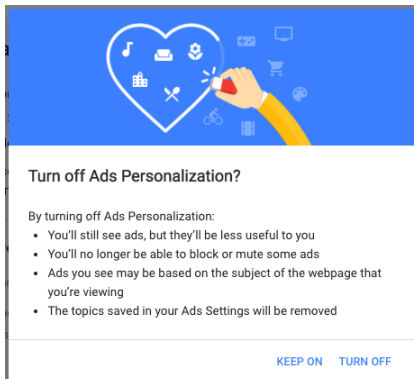
7. Click "Manage your ads settings."



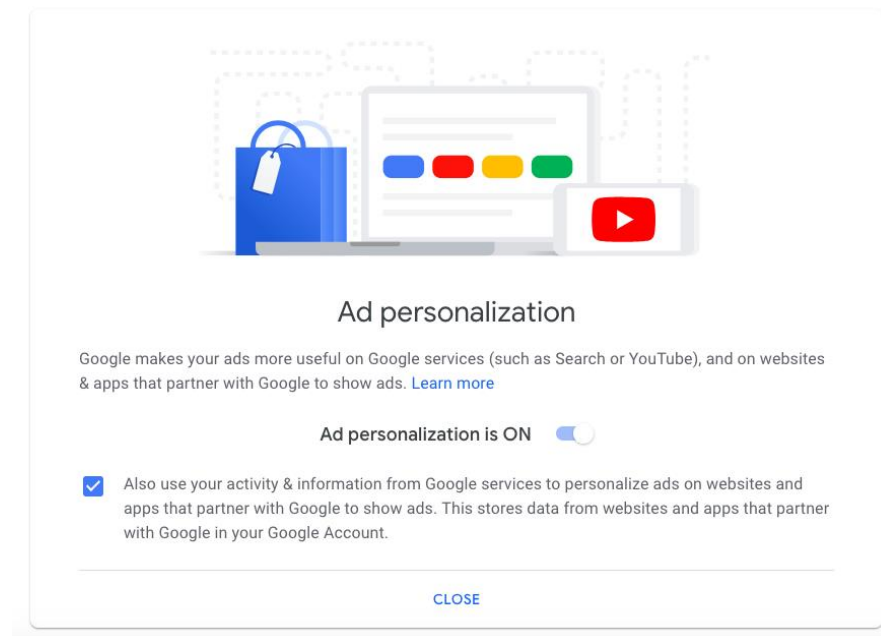
8. Turn “Ads Personalization” off. It was turned on by default in the initial view.



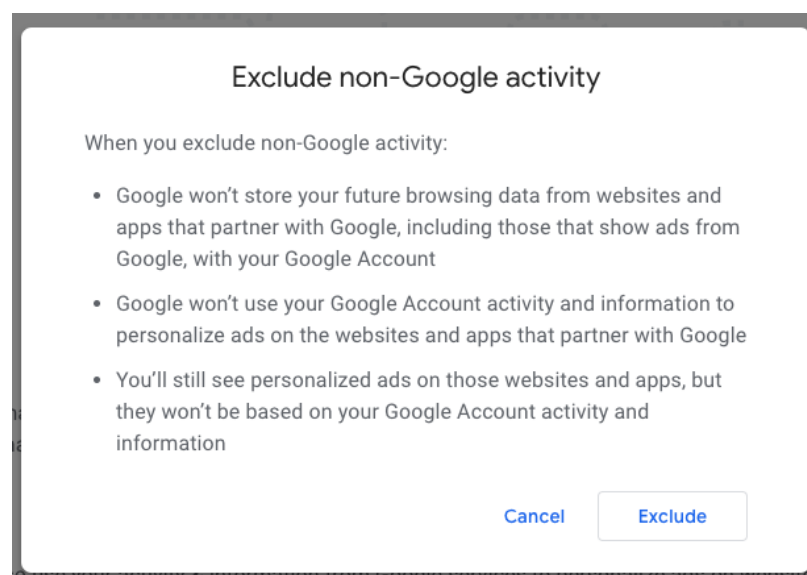
9. Click “Turn off”



Earlier versions of Google's ads settings page allowed users to control tracking on third party sites and ads based on Google account activity separately. As of 2016, these two settings are intertwined. When a user with Ads Personalization switched off turns the setting back on, Google automatically checks the box that allows the company to store data from third party sites and apps in the user's account and use this combined data for ads personalization.



To disable the combination of third party tracking data with personal account information, users had to uncheck this box and click "Exclude" on the following prompt.



It is likely that many users – especially those who use desktop email clients - never saw Google's notification about its new privacy policy, and never had the opportunity to opt out of Google's

expanded data collection. Those who did not receive the notification had to manually navigate to the Ads Personalization settings to opt out of the new data collection policy.<sup>17</sup>

### *Hidden Information about Data Sources*

Google's notifications and ads personalization settings obscure the fact that sites that serve Google ads are only a fraction of the sites that send users' browsing data back to Google. The ads personalization page only makes a vague reference to collecting data from "websites and apps that partner with Google."<sup>18</sup> The ads settings page mentions the "2+ million websites that partner with Google to show ads," but makes no mention of data collection from other sites.<sup>19</sup>

A footnote linked from Google's privacy policy (not directly accessible from the ads settings page) offers deeper insight – falling short of total transparency – into the breadth of Google's data-gathering operation. It states in full:

“This activity might come from your use of Google products like Chrome Sync or from your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These products share information about your activity with Google and, depending on [your account settings](#) and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.”<sup>20</sup>

Although Google's notification to users about its new privacy settings emphasized data sharing with sites that serve ads, this definition buried in its privacy policy makes clear that Google also gleans user data from sites and apps that use *any* Google service. This omission is hardly trivial; Google Analytics is present on more than 13 million internet domains.<sup>21</sup>

Google services that entitle the company to user data may also include the Application Programming Interfaces (APIs) that Google distributes to Android app developers through Google Play Services, which are governed by the same privacy policy as Google's web properties.<sup>22</sup> Even third-party apps (those not developed by Google itself) can contribute to the user data that Google collects, combines with personal information, and uses for advertising purposes. For example, a 2015 study demonstrated that the Facebook app for Android, which uses Google APIs, sends users' email, name, username, and location to Google. The Facebook iOS app did not send any data to Apple.<sup>23</sup>

---

<sup>17</sup> <http://deliddedtech.com/2016/07/11/google-adds-new-options-regarding-data-collection-privacy-for-ads/>

<sup>18</sup> <https://adssettings.google.com/u/0/authenticated>, <https://google.com/ads/preferences>

<sup>19</sup> <https://google.com/ads/preferences>

<sup>20</sup> <https://policies.google.com/privacy#footnote-other-sites>, <https://www.google.com/policies/privacy/example/your-activity-on-other-sites-and-apps.html> (2016 version)

<sup>21</sup> <https://www.datanyze.com/market-share/web-analytics>

<sup>22</sup> [https://developers.google.com/terms/#a\\_google\\_privacy\\_policies](https://developers.google.com/terms/#a_google_privacy_policies)

<sup>23</sup> <http://techscience.org/a/2015103001/index.php#Demonstration>

## Google's Prior Statements Regarding Doubleclick Data and User Privacy

The combination of user data from Google accounts with data from third party sites and apps realized the fears advanced by consumer advocates when Google acquired Doubleclick, the technology it uses to serve ads to its Display Network, in 2008. Until 2016, Google stated that the company would solicit user consent before combining Doubleclick data with information that Google deems ‘personally identifiable.’<sup>24</sup> The 2016 privacy policy change removed this clause, allowing Google to create ‘super-profiles’ that track users everywhere.

Doubleclick tracks user data using “cookies,” or small text files that it stores on users’ browsers. Google places a Doubleclick cookie on an individual’s browser when she interacts with the Doubleclick server, usually by visiting a page that shows Doubleclick ads.<sup>25</sup> Cookies can communicate with the server about how many times a user has seen a particular ad, but they can also track users across the web to determine their particular interests – so Doubleclick will serve ads about sports to people who spend a lot of time on the ESPN and NFL websites, and ads about clothing to people who browse fashion blogs and department store websites, even when they’re viewing unrelated content.<sup>26</sup>

During the acquisition, Google faced opposition from consumer advocates and scrutiny from the Federal Trade Commission. While Google’s competitors focused on the unfair market advantage that the acquisition would create, consumer advocates focused on privacy concerns raised by combining Doubleclick and Google’s data resources. In a letter, the New York State Consumer Protection Board said, “[t]he combination of Doubleclick’s Internet surfing history generated through consumers’ pattern of clicking on specific advertisements, coupled with Google’s database of consumers’ past searches, will result in the creation of ‘super-profiles,’ which will make up the world’s single largest repository of both personally and non-personally identifiable information.”<sup>27</sup>

Google sought to reassure the the FTC, Congress, and the general public that the acquisition would not sacrifice user privacy. Google’s General Counsel, Nicole Wong, said that the merged company would give users “real choices that are transparent to them” regarding data collection.<sup>28</sup> In a statement before Senate Judiciary Subcommittee on Antitrust, Competition Policy, and Consumer rights, Chief Legal Officer David Drummond said, "DoubleClick is already extremely protective of privacy. In fact, it does not own and has very limited rights to use any of the data it processes on behalf of its publisher and advertiser clients."<sup>29</sup> In response to questioning from the committee,

---

<sup>24</sup> <https://www.google.com/policies/privacy/archive/20111020-20120301/>. Google defines personally-identifiable information as “information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google, such as information we associate with your Google account.” (<https://www.google.com/intl/en/policies/privacy/key-terms/#toc-terms-info>). As Jones-Harbour points out in her dissent and more recent scholarly work argues, this is only a subset of the information that could be used to identify a user. IP addresses, computer battery status, and even the position of a browser window on the screen can be used to identify an individual.

([http://randomwalker.info/publications/OpenWPM\\_1\\_million\\_site\\_tracking\\_measurement.pdf](http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf))

<sup>25</sup> <https://support.google.com/adsense/answer/2839090?hl=en>

<sup>26</sup> <https://www.theguardian.com/technology/2012/apr/23/DoubleClick-tracking-trackers-cookies-web-monitoring>

<sup>27</sup> Statement of Marc Rotenberg, Executive Director Electronic Privacy Information Center; Committee on Senate Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights; September 27, 2007

<sup>28</sup> <http://articles.latimes.com/2007/apr/17/business/ft-privacy17>

<sup>29</sup> <https://www.judiciary.senate.gov/imo/media/doc/Drummond%20Testimony%2009272007.pdf>

Drummond reiterated that DoubleClick’s “data is owned by the customers – publishers and advertisers – and DoubleClick or Google can’t do anything with it.”<sup>30</sup>

The FTC declined to intervene in the privacy issue, arguing that “the Commission lack[s] legal authority to require conditions to this merger that do not relate to antitrust,” opting instead to promote a set of voluntary self-regulation principles for companies that collect user data.<sup>31</sup> These principles have induced little change in company behavior.

Regarding the competitive advantage granted to Google by combining its user data with data obtained through Doubleclick tracking cookies, the Commission simply pointed out that under its contracts at the time, Doubleclick had limited access to user data.

In a dissenting statement, Commissioner Pamela Jones-Harbour argued that the combination of Doubleclick and Google user data raised both antitrust and privacy concerns within the purview of the commission:

“The parties claim to place a high value on protecting consumer privacy. In various fora, both public and private, senior corporate officials have offered assurances that the combined firm will not use consumer data inappropriately. But charged as I am with protecting the interests of consumers, I am uncomfortable accepting the merging parties’ nonbinding representations at face value. The truth is, we really do not know what Google/DoubleClick can or will do with its trove of information about consumers’ Internet habits. The merger creates a firm with vast knowledge of consumer preferences, subject to very little accountability.”<sup>32</sup>

Google proceeded to build tandem user profiles based on account data and browsing data, aided by information that Google does not deem “personally identifying,” such as partial IP addresses.<sup>33</sup> In 2015, Google earned more than \$15 billion in advertising revenue from ads displayed on sites and apps using Doubleclick technology.<sup>34</sup>

Now, Google can combine Doubleclick data with other browsing activity as well as personal information, making it harder for users to preserve their privacy and harder for other advertisers to compete.

---

<sup>30</sup> <https://www.judiciary.senate.gov/imo/media/doc/Drummond%20Testimony%2009272007.pdf>

<sup>31</sup> [https://www.ftc.gov/system/files/documents/public\\_statements/418081/071220googledc-commstmt.pdf](https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf)

<sup>32</sup> [https://www.ftc.gov/sites/default/files/documents/public\\_statements/statement-matter-google/DoubleClick/071220harbour\\_0.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/DoubleClick/071220harbour_0.pdf)

<sup>33</sup> Commissioner Jones-Harbour’s dissent predicted this approach; pointing out that an IP address from a session cookie could be matched with an IP address from a longer-term account cookie to associate an individual with server log records.

<sup>34</sup> Calculated from quarterly earnings from Google Network Members’ websites. Available at:

[https://abc.xyz/investor/news/earnings/2015/Q1\\_google\\_earnings/](https://abc.xyz/investor/news/earnings/2015/Q1_google_earnings/),

[https://abc.xyz/investor/news/earnings/2015/Q2\\_google\\_earnings/](https://abc.xyz/investor/news/earnings/2015/Q2_google_earnings/),

[https://abc.xyz/investor/news/earnings/2015/Q3\\_google\\_earnings/](https://abc.xyz/investor/news/earnings/2015/Q3_google_earnings/),

[https://abc.xyz/investor/news/earnings/2015/Q4\\_google\\_earnings/index.html](https://abc.xyz/investor/news/earnings/2015/Q4_google_earnings/index.html)



## *2010 Consent Decree*

Google's quiet rollout of its mid-2016 privacy policy, ads settings language that obscures the scope of the company's data gathering, and the move from an opt-in to an opt-out model for the handling of tracking cookie data may all violate a 2010 consent decree that the FTC reached with Google after an earlier invasion of users' privacy.

Commissioner Jones-Harbour's view that Google must be formally bound to standards for user privacy was vindicated in 2010 when the firm came under FTC scrutiny again for automatically collecting and combining user data from Gmail, Picasa, Google Reader, and other services in the rollout of a short-lived social network called Google Buzz.

The Commission found Google to be in violation of the FTC Act for misrepresenting what it planned to do with the user data that it collected through Gmail and for failing to obtain consent to use the data in a new way.<sup>35</sup> The FTC also found that Google's actions violated the US-EU Safe Harbor Framework, which requires that entities that collect personal information provide users with notice about how the data will be used and the ability to opt out easily.

Following an investigation, the FTC issued a consent decree ordering Google to truthfully represent the way it gathers and uses information, obtain affirmative consent separate from the privacy policy for user participation in new data sharing, and develop internal procedures for mitigating adverse effects of future privacy changes.<sup>36</sup>

Consumer advocates at the Electronic Privacy Information Center (EPIC) accused Google of violating this consent decree in 2012, when the firm announced that it would combine data obtained from users' search histories with personal information gathered from other Google services. In a complaint, EPIC argued that by combining data across services, Google "misrepresent[ed] the extent to which it maintains and protects privacy and confidentiality of covered information," and that the firm "fail[ed] to obtain affirmative consent from users prior to sharing their information with third parties."<sup>37</sup> Further information on the EPIC complaint is set out in the attachment to this paper.

Specifically, the consent decree ordered that:

[R]espondent, prior to any new or additional sharing by respondent of the Google user's identified information with any third party, that: 1) is a change from stated sharing practices in effect at the time respondent collected such information, and 2) results from any change, addition, or enhancement to a product or service by respondent, in or affecting commerce, shall:

A. Separate and apart from any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, clearly and prominently disclose: (1) that the Google user's information will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for respondent's sharing; and

---

<sup>35</sup> <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf>

<sup>36</sup> <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf>

<sup>37</sup> <https://epic.org/privacy/ftc/google/EPIC-Complaint-Final.pdf>

B. Obtain express affirmative consent from the Google user to such sharing.<sup>38</sup>

The 2012 EPIC complaint focused on Google's failure to allow users to opt out of combining their search data with other information. The 2016 policy change gave users more freedom to provide consent, but the notification that existing users received did not "clearly and prominently disclose...the identity of specific categories" of third party sites and apps with which Google now shares data.

This would not be the first time that Google has faced legal scrutiny for being too vague about its privacy policies. A 2013 official study by the Dutch Data Protection Authority argued:

Because Google does not provide specific enough information about the types of data it collects from its various services and about the types of data it combines for the purposes of personalising requested services, product development, displaying targeted ads and website analytics, Google is acting in breach of the provisions of Articles 33 and 34 of the Wbp<sup>39</sup>

---

<sup>38</sup> <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf>

<sup>39</sup> [https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn\\_privacy/en\\_rap\\_2013-google-privacypolicy.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf)

## Motivations: Context-Aware Apps and Advertisements

The 2016 privacy policy allows Google to collect user data from sites and apps even when they are not actively sending data to their devices. This “context data” – all of the information surrounding users’ structured interactions with the internet – is the future of computing and online advertising.<sup>40</sup>

*2012: Combining user data across Google Services makes Google Now possible*

EIPC’s 2012 complaint targeted a privacy policy change that allowed Google to combine users’ search histories with personal information obtained from other Google services.<sup>41</sup> Google announced the change two months before it took effect to widespread outcry. Privacy advocates and commentators condemned Google for its failure to allow users to opt out of this unprecedented invasion of privacy.<sup>42</sup>

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.

### Relevant changes to Google’s privacy policy, March 2012

Perhaps as a concession to concerned parties, Google maintained its commitment to keep Doubleclick data separate from personal information in the new privacy policy. An article published in *The Guardian* six weeks after the new policy took effect bluntly stated that “Your browsing behavior will never be linked to your Gmail account.”<sup>43</sup>

In the fracas over user privacy and advertising, many commenters overlooked the role of the privacy policy change in a new service: Google Now (which has since been replaced by Google Assistant).

The 2012 privacy policy change paved the way for the debut of the Google Now app three months later.<sup>44</sup> Like its descendant, Google Assistant, Google Now combined data from users’ activity across Google products with “contextual” information such as location and activity to provide content tailored to users’ commutes, travel plans, activities, and interests. By combining data from search histories with email content and other data, the app “aim[ed] to seek out information for users before they even think of typing it into the search box.”<sup>45</sup>

Google Now made visible how much the search giant can learn about its users:

---

<sup>40</sup> <http://kvadrevu.com/thinking-about-context-aware-ads/> , <http://qz.com/205689/context-this-is-what-comes-after-search/>

<sup>41</sup> [https://www.washingtonpost.com/business/technology/faq-googles-new-privacy-policy/2012/01/24/gIQA8w8GOQ\\_story.html](https://www.washingtonpost.com/business/technology/faq-googles-new-privacy-policy/2012/01/24/gIQA8w8GOQ_story.html)

<sup>42</sup> <http://outfront.blogs.cnn.com/2012/03/01/googles-new-privacy-policy-accept-or-decline-and-be-banished/>, [https://www.washingtonpost.com/business/technology/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQA8w8GOQ\\_story.html](https://www.washingtonpost.com/business/technology/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQA8w8GOQ_story.html)

<sup>43</sup> <https://www.theguardian.com/technology/2012/apr/23/DoubleClick-tracking-trackers-cookies-web-monitoring>

<sup>44</sup> <https://www.yahoo.com/news/what-android-users-should-know-about-the-jelly-bean-4-1-update.html?ref=gs>

<sup>45</sup> <http://time.com/google-now/>

The part that clearly disturbs some people about Google Now is the data collection that is involved in making it work: the tracking of your web searches, your calendar appointments, your location via GPS, the photos you have posted, the flights you are preparing to take, and so on. There's no question that this is invasive.<sup>46</sup>

Google Now users had the ability to modify their privacy settings to customize the amount of data that they share with the app, but “but denying it access to your life robs it of its purpose.”<sup>47</sup> The relationship between the app's usefulness and the volume of user data that it could access allowed Google Now to function as a disincentive for restrictive privacy settings. Moreover, Google's post-March 2012 privacy settings allow it to combine this information for its own purposes behind the scenes, even if the user does not request to view the aggregated information through the Google Now app.

Beyond incentivizing users to grant Google access to personal information, Google Now also became a source of information in itself by developing a detailed model of users' daily habits. “Context-aware” apps like Google Now help companies fill in the details of a user's day when she isn't actively browsing the web. “If a developer wants to know everything that a user is doing, [they] need to know the user's context and create a narrative of the user's day,” the product manager for Intel's context-sensing software said in 2010.<sup>48</sup>

Gaining access to richer “context data” also motivated Google's acquisition of traffic and mapping company Waze in 2013<sup>49</sup> and home automation company Nest in 2014.<sup>50</sup> Both technologies allow the company to know more about how users live their lives, and to serve ads based on that data. Nest caused a minor controversy shortly after its acquisition by reneging on an earlier promise to keep its data separate from Google users profiles.<sup>51</sup>

### *2015 and 2016: Collecting context data from third party apps*

In 2015, Google announced that it would open Google Now to 40 popular apps like Uber, AirBnB, and Spotify.<sup>52</sup> While Google assured users that it would not share their personal context data with these third party apps, data does flow freely in the other direction. In order for third party app integrations to work, Google Now sucks in user data from linked apps – and it can use this data in any way that conforms with Google's privacy policy.<sup>53</sup>

---

<sup>46</sup> <https://gigaom.com/2013/05/03/the-google-now-dilemma-yes-its-kind-of-creepy-but-its-also-incredibly-useful/>

<sup>47</sup> <http://www.telegraph.co.uk/technology/mobile-app-reviews/10032788/Google-Now-for-iOS-review-straddling-the-creepy-line.html>

<sup>48</sup> <http://www.intelfreepress.com/news/contextual-sensing-smartphone-learning/9467/>

<sup>49</sup> <https://techcrunch.com/2013/06/11/behind-the-maps-whats-in-a-waze-and-why-did-google-just-pay-a-billion-for-it/>

<sup>50</sup> <http://arstechnica.com/gadgets/2014/01/the-battle-for-the-home-why-nest-is-really-googles-new-smart-home-division/>

<sup>51</sup> <http://www.techhive.com/article/2366987/just-kidding-says-nest-we-are-totally-sharing-your-data-with-google.html>

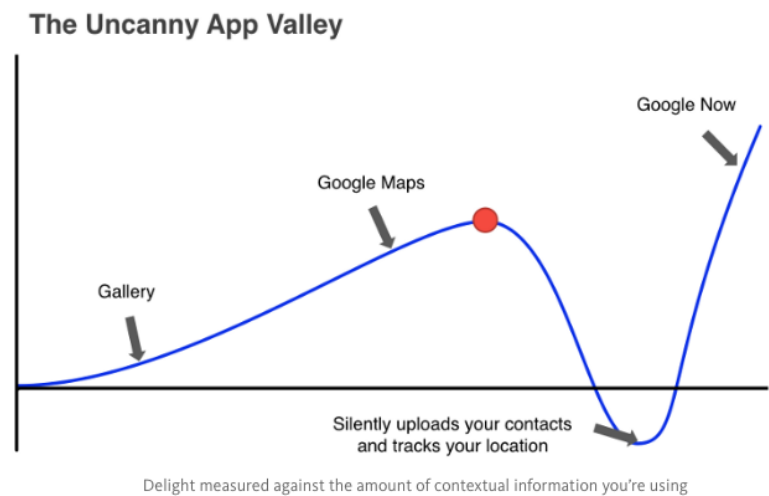
<sup>52</sup> <https://search.googleblog.com/2015/01/google-app-update-get-now-cards-from.html>

<sup>53</sup> <http://www.csmonitor.com/Technology/2015/0130/Google-Now-powers-up-by-pulling-in-info-from-other-apps>, <http://blogs.wsj.com/digits/2015/01/30/google-now-will-suck-in-outside-app-data/>

The 2015 data sharing announcement already afforded Google the ability to gather user data from third party apps that entered into partnerships with Google Now, but the 2016 changes to the privacy policy give Google the freedom to go farther, gathering data from third party apps that are only loosely tied to Google.

Two days after it changed its privacy policy governing data collection from third party apps and sites, Google rolled out the Awareness API for Android developers.<sup>54</sup> The API gathers a wide variety of context data, including the local time, specific location (including a description of the place type), detected physical activity, device state (such as whether the headphone jack is in use), nearby landmarks, and ambient conditions such as weather.

In a July 14<sup>th</sup> Medium article, an “Android Developer Advocate” employed by Google made the case for incorporating the API into “delightful, intelligent apps,” and coached developers on how to use context data without disturbing users.<sup>55</sup> He advocated for more data collecting on the service of greater responsiveness, suggesting that third party developers should maximize both data collection and “delight” in the mode of Google Now.



In 2016, Google introduced Google Assistant, which augmented the basic functionality

**A Medium post by an Android developer advocate suggests that Google Now maximizes data collection and “delight.”**

of Google Now with deeper artificial intelligence that drew upon past conversations and interactions with the software.<sup>56</sup> Like Google Now, Google Assistant pulls in data from the users' web and app activity and can be integrated with third party apps and services.<sup>57</sup> The software relies on broad data collection in order to tailor its responses to users, a practice that *Gizmodo* deemed “a privacy nightmare.”<sup>58</sup>

Unlike Google Now, Assistant is automatically integrated into some Google devices and services, and could be enabled without the user's knowledge. In February 2019, Google announced that voice interactions with Google Assistant would soon become available on the company's Nest Guard

<sup>54</sup> <http://technews.co/2016/06/30/google-unveils-new-awareness-api-to-help-developers-create-intelligent-and-context-aware-apps/>

<sup>55</sup> <https://medium.com/google-developers/using-the-awareness-api-for-android-a185b05e7254#.ehackvav1>

<sup>56</sup> <https://www.cnet.com/how-to/the-difference-between-google-now-and-google-assistant/>

<sup>57</sup> [https://support.google.com/assistant/answer/7126196?p=assistant\\_privacy&visit\\_id=1-636112016868512038-512077472&rd=2](https://support.google.com/assistant/answer/7126196?p=assistant_privacy&visit_id=1-636112016868512038-512077472&rd=2),

<https://support.google.com/googlehome/answer/7126338?co=GENIE.Platform%3DAndroid&hl=en>

<sup>58</sup> <https://gizmodo.com/googles-ai-plans-are-a-privacy-nightmare-1787413031>

home security device.<sup>59</sup> The company had not previously disclosed that the device had a microphone.<sup>60</sup>

### 2016: "Closing the Loop" across devices

With an emphasis on voice interactions, Assistant seeks to provide a personalized experience across mobile phones, internet of things devices (like Google Home and Nest), and PCs. Identifying the same user across devices is essential to providing the "personalized experience" that Google seeks to create with Google Assistant. It is also essential to surgically precise ad targeting.

Associating browsing data with users' profiles allows Google to monitor users across devices. In



September 2016, less than three months after the privacy policy change that combined Doubleclick tracking cookies with personal profile information, Google announced a new set of services that allow advertisers to “close the loop” with cross-device remarketing.<sup>61</sup> For example, Google can now determine which signed-in users saw an ad on her phone and purchased the advertised product on her desktop computer.<sup>62</sup>

Previously, cookies (on computers) and Advertising IDs (on mobile devices) tracked user activity and built profiles for browsing behavior on each device, but these data stores were siloed off from one another. Google’s old privacy policy effectively forbade the company from associating a user’s activity on a smartphone with the same user’s activity on a desktop computer for advertising purposes. Under the new privacy policy, Google can associate user activity on any app or site using Google services with a user’s private account, unifying activity data across all of a user’s devices.<sup>63</sup>

Until 2018, Google did not disclose that allowing the company to combine data from third party apps and sites with personal account data would allow the company to track users across their devices. Only after the company revised its policies to comply with the European General Data Protection Regulation did the company mention cross-device tracking in its ads settings. Even now, this language is only visible to users who elect to turn on ads personalization. Users who already have ads personalization turned on receive no information about cross-device tracking.

Two of Google’s advertising “innovations” announced in 2016 draw upon this new capability. One of these services, billed as “Cross-device remarketing for Google Display Network and Doubleclick

<sup>59</sup> <https://www.blog.google/products/assistant/nest-secure-google-assistant/>

<sup>60</sup> <https://www.csoonline.com/article/3336227/security/nest-secure-had-a-secret-microphone-can-now-be-a-google-assistant.html>

<sup>61</sup> <https://adwords.googleblog.com/2016/09/New-Digital-Innovations-to-Close-the-Loop-for-Advertisers.html>

<sup>62</sup> <https://techcrunch.com/2016/09/26/google-ads/>

<sup>63</sup> See “Google Stealthily Enables ‘Super-Profiles’” (proprietary memo), September 16, 2016.

Bid Manager,” allows advertisers to track users’ activity across all of the devices where they are signed in to Google and to serve ads even on machines where they have not looked at related content. In its blog, Google provided the example of a user who searches for Halloween costume ideas on her phone in the morning, and then sees ads for a costume shop on her desktop computer in the afternoon and her iPad at night.

The second relevant “innovation” allows Google to combine context data about a user’s location with information in a user’s advertising profile to drive customers to physical stores. This service combines background requests for mobile users’ physical location with information about the content on their screens to serve users ads with directions to the nearest store containing relevant products.

Even more disturbingly, Google then reports on the efficacy of these ads by tracking users’ movements and cross-referencing with Google Maps data to determine with “99% accuracy” whether or not a user visited the advertised store.<sup>64</sup> Google can provide its advertising customers with detailed information about the ‘paths’ that users take between viewing an ad and making a conversion, even if the store visit is captured by different device than the one that served the ad.<sup>65</sup>

By combining browsing and web activity data into a user’s Google account, the company can determine which signed-in users saw an ad on one device and purchased the advertised product on another.<sup>66</sup> The company has also filed a patent application that could allow it to track signed-out users by passing a temporary tracking code between devices for the purposes of cross-device remarketing and conversion tracking.<sup>67</sup>

In its blog, Google notes that “Only Google can deliver this level of precision and scale [of user data].” With its ‘super-profiles’ created by combining Doubleclick and Google Account data across devices, this is certainly true.

---

<sup>64</sup> <https://static.googleusercontent.com/media/www.google.com/en/us/adwords/start/marketing-goals/pdf/white-paper-bridging-the-customer-journey.pdf>

<sup>65</sup> <https://support.google.com/adwords/answer/6359141>, <https://www.Doubleclickbygoogle.com/articles/cross-device-conversion-metrics-come-DoubleClick/>

<sup>66</sup> <http://marketingland.com/google-cross-device-remarketing-launches-192819>

<sup>67</sup> <http://pdfaiw.uspto.gov/.aiw?Docid=20160234203>



## Appendix: Timeline of Google's Interest-Based Advertising Policies



[Privacy Center](#)

[Privacy Overview](#)

[Privacy Policy](#)

[Privacy FAQ](#)

[Privacy Glossary](#)

[Privacy Blogs](#)

[Terms of Service](#)

Find on this site:

Search

### Advertising and Privacy

We serve search text ads via [AdWords](#) on [google.com](#), and we also serve contextual and placement-targeted text and display ads on the [Google content network](#) ([AdSense](#)). To protect privacy, we follow three principles when we serve ads:

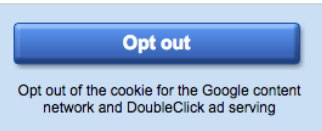
- **Transparency** – We provide detailed information about our advertising policies and practices.
- **Choice** – We offer an opt-out for advertising cookies.
- **No personally identifiable information** – We don't collect or serve ads based on personal information without your permission.

The [Google Privacy Policy](#) describes how we treat personal information in Google's products and services, including information provided when using or interacting with our advertising services. In addition, the [Privacy Policy for Google ads and the Google content network](#) describes our privacy practices relating to our advertising services.

### Advertising Cookie Opt-out

Google uses cookies to serve more relevant ads. Learn more about [how Google uses advertising cookies](#).

Anyone may opt out of the DoubleClick cookie (for both the Google content network and DoubleClick ad serving) at any time by clicking the button above. In addition, Google allows third party advertisers to serve ads on the Google content network. Using a tool created by the [Network Advertising Initiative](#), you can [opt out](#) of several third party ad servers' and networks' cookies simultaneously. (Google also uses cookies for Google Analytics and conversion tracking. Read more about this in our [FAQ](#) below.)



Pre-2009: Google serves ads based on context, such as current web searches or active page content. Opting out disables the Doubleclick cookie.



### Make the ads you see on the web more interesting

Many websites, such as news sites and blogs, partner with us to show ads on their sites. To see ads that are more related to your interests, edit the interest categories below, which are based on sites you have recently visited. [Learn more](#)

Your interests are associated with an advertising cookie that's stored in your browser. If you don't want us to store your interests, you can opt out below.

Watch our video:

[Ads Preferences explained](#)



Ads Preferences affect ads that Google shows on other websites.

<b>Your interests</b>	Below you can edit the interests that Google has associated with your cookie:												
	<table><thead><tr><th>Category</th><th></th></tr></thead><tbody><tr><td>Automotive</td><td><a href="#">Remove</a></td></tr><tr><td>Computers &amp; Electronics - Consumer Electronics - Personal Electronics</td><td><a href="#">Remove</a></td></tr><tr><td>News &amp; Current Events - Technology News</td><td><a href="#">Remove</a></td></tr><tr><td>Sports - Golf</td><td><a href="#">Remove</a></td></tr><tr><td>Travel - Air Travel</td><td><a href="#">Remove</a></td></tr></tbody></table>	Category		Automotive	<a href="#">Remove</a>	Computers & Electronics - Consumer Electronics - Personal Electronics	<a href="#">Remove</a>	News & Current Events - Technology News	<a href="#">Remove</a>	Sports - Golf	<a href="#">Remove</a>	Travel - Air Travel	<a href="#">Remove</a>
Category													
Automotive	<a href="#">Remove</a>												
Computers & Electronics - Consumer Electronics - Personal Electronics	<a href="#">Remove</a>												
News & Current Events - Technology News	<a href="#">Remove</a>												
Sports - Golf	<a href="#">Remove</a>												
Travel - Air Travel	<a href="#">Remove</a>												
	<a href="#">Add interests</a> Google does not associate sensitive interest categories with your ads preferences.												
<b>Opt out</b>	Opt out if you prefer ads not to be based on the interest categories above. <a href="#">Opt out</a> When you opt out, Google disables this cookie and no longer associates interest categories with your browser.												

2009: Google launches interest-based advertising the Doubleclick network and introduces the “Ads Preferences” manager for editing or opting out of interest-based profiles.

## Ads Preferences

### ▼ Ads on Search and Gmail

Blocked advertisers

Opt out

### ▶ Ads on the web

#### Ads on Search and Gmail

With personalized ads, we can improve your ad experience by showing you ads related to websites you visit, recent searches and clicks, or information from your Gmail inbox.

Google tries to show you the most relevant ads, whether or not you're opted in to seeing personalized ads. While we often match ads with specific pages (based on the page content or the search terms you enter), additional information helps us personalize your ads. [Learn more](#)

▶ [Watch a video about ads personalization](#)

#### Why these ads?

Find out why we showed you these ads when you searched for **microsoft**. Below, you can also choose to block specific advertisers' ads if you don't find them helpful.

▼ **Microsoft Support | microsoft-support.fixnow.us - microsoft-support.fixnow.us** - [Block this advertiser](#)

##### Search terms

This ad matches terms similar to the ones you entered.

▶ **Buy from Microsoft® Store - Official Site. Download Software.** - [www.microsoftstore.com/US\\_Online\\_Store](#) - [Block this advertiser](#)

▶ **Microsoft Tech Support - www.myphonesupport.com/Microsoft/** - [Block this advertiser](#)

### ▼ Ads on the web

Opt out

Many websites, such as news sites and blogs, partner with us to show ads to their visitors. To see ads that are more related to you and your interests, edit the categories below, which are based on sites you have recently visited. [Learn more](#)

Your interests are associated with an advertising cookie that's stored in your browser. If you don't want us to store your interests, you can opt out below. Your ads preferences only apply in this browser on this computer. They are reset if you delete your browser's cookies.

▶ [Watch a video: Ads Preferences on Google Display Network explained](#)

#### Your categories

Below you can review a summary of the interests that Google has associated with your cookie.

Computers & Electronics - Consumer Electronics - Gadgets & Portable Electronics - E-Book Readers [Remove](#)

Games - Computer & Video Games - Sports Games - Sports Management Games [Remove](#)

Games - Online Games [Remove](#)

News - Sports News [Remove](#)

Reference - Libraries & Museums - Museums [Remove](#)

Sports - Team Sports - American Football [Remove](#)

Sports - Team Sports - Soccer [Remove](#)

[Add or edit interests](#)

#### Your demographics

Below you can review the inferred demographics that Google has associated with your cookie. We infer your age and gender based on the websites you've visited.

Age: 25-34

Gender: Male

groovyPost.com [Remove](#)  
[Remove](#)






2011: Google expands interest-based advertising to its own sites and products and introduces an updated Ads Preferences manager, allowing users to control Google activity profiles and Doubleclick cookie data separately



## Ads Settings

### Settings for Google ads

Ads enable free web services and content. These settings help control the types of Google ads you see.

	Ads on Google	Google ads across the web <sup>?</sup>
	<div> Search</div> <div> Gmail</div> <div> YouTube</div> <div> Maps</div>	<div></div> <div>Google ads across the web</div>
Gender	Female <a href="#">Visit your Google Profile</a>	Female Based on your Google profile <sup>?</sup>
Age	18-24 <a href="#">Visit your Google Profile</a>	18-24 Based on your Google profile <sup>?</sup>
Languages	N/A	English <a href="#">Edit</a> Based on the websites you've visited
Interests	Unknown <a href="#">Edit</a> From your previous activity on Google	Celebrities & Entertainment News, and 20 more <a href="#">Edit</a> Based on the websites you've visited
Advertisers' campaigns you've blocked <sup>?</sup>	None From your blocking activity	N/A
Opt-out settings	<a href="#">Opt out of interest-based ads on Google</a>	<a href="#">Opt out of interest-based Google ads across the web</a>

2013: Google renames “Ads Preferences” to “Ads Settings” and redesigns the page to reflect the fact that user activity across all Google services are consolidated into a single profile. Doubleclick and Google profiles remain separate.

#### ◦ Cookies and anonymous identifiers

We [and our partners](#) use various technologies to collect and store information when you visit a Google service, and this may include sending one or more [cookies](#) or [anonymous identifiers](#) to your device. We also use cookies and anonymous identifiers when you interact with services we offer to our partners, such as [advertising services](#) or Google features that may appear on other sites. [Our Google Analytics product helps businesses and site owners analyze the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google Analytics information is linked, using Google technology, with information about visits to multiple sites.](#)

2015: Google quietly updates its privacy policy to acknowledge that it combines Google Analytics information with Doubleclick cookie data, but keeps the Ads Settings page the same.



These settings apply across your browsers and devices when you're signed in to Google as [redacted]@gmail.com

Ads Settings works differently when you sign in to multiple accounts. [Learn more](#)



## Ads Personalization

☒ ON

Make the ads you see more useful to you when using:

- Google services (ex: Search, YouTube)
  - 2+ million non-Google websites and apps that partner with Google to show ads
- ☒ Also use Google Account activity and information to personalize ads on these websites and apps and store that data in your Google Account

What are the 2+ million websites and apps that partner with Google to show ads?



What personal information does Google give to partners?



## Your topics

☐ Parenting

+ NEW TOPIC

WHERE DID THESE COME FROM?

### Include additional activity?

By including additional activity, Google will:

- Include your browsing data from websites and apps that partner with Google, including those that show ads from Google, in your Google Account
- Store that data with other data in your Google Account based on your [Activity Controls](#) preferences
- Use Google Account activity to make ads across the web more relevant for you, improve the relevance of ads on those websites and apps, and improve Google services

This setting applies across all of your signed-in devices and across all Google services.

CANCEL INCLUDE



### Turn on Ads Personalization?

This setting gives Google permission to use your Google Account activity and information on Google services (ex: Search, YouTube) as well as your browsing data from websites and apps that partner with Google to:

- Show you ads that are relevant to you
- Improve the relevance of ads on those websites and apps

Google will use that same data to personalize ads on those websites and apps. You can turn this option off by unchecking the box after Ads Personalization is turned on.

This setting applies across all of your signed-in devices and across all Google services.

KEEP OFF TURN ON

2016: Google rebrands “Ads Settings” as “Ads Personalization” and consolidates users’ Google profiles with tracking data from Doubleclick and other Google services. By default, accounts are set to track users across Google Services and all third party sites and apps that use Google for advertising, analytics, video, and more. Users have the option to exclude their Google account information from their advertising profiles, but cannot control when and where Google tracks them without disabling interest-based advertising entirely.



## Ad personalization

Google makes your ads more useful on Google services (such as Search or YouTube), and on websites & apps that partner with Google to show ads. [Learn more](#)

Ad personalization is ON ☒

- ☒ Also use your activity & information from Google services to personalize ads on websites and apps that partner with Google to show ads. This stores data from websites and apps that partner with Google in your Google Account.

[CLOSE](#)



## Turn on personalization

When you turn on ad personalization, you give Google permission to show you ads based on your activity on:

- Google services (such as Search or YouTube)
- Websites and apps that partner with Google to show ads

This info helps Google show ads that may be useful to you. You can choose to exclude info from websites and apps through "MORE OPTIONS."

Personalization applies to [redacted]@gmail.com across your devices. For example, if you visit a travel website on your home computer in the morning, you might see ads about train tickets on your phone later that day.

[Keep off](#)

[Turn on](#)

2018: To comply with the European General Data Protection Regulation, Google rewrites its privacy policy, pushes "privacy checkups," and allows new users to opt out of data collection at sign-up. For the first time, Google explicitly discloses that it tracks users across devices, but only when users turn on ads personalization for the first time. Maximally-invasive privacy settings remain on by default.

# BACKGROUND TO THE 2011 FTC CONSENT ORDER RE: GOOGLE BUZZ

*1 March 2019*

## FTC Consent Orders

A consent order issued by the Federal Trade Commission ("FTC") is a settlement agreement with the party under investigation. Under Section 5(b) of the FTC Act, the FTC may investigate conduct and subsequently challenge "unfair or deceptive act[s] or practice[s]" through an administrative adjudication by issuing a complaint. If the respondent elects to settle the FTC's charges, it may sign a consent agreement (without admitting liability) and waive all right to judicial review. If the FTC accepts the proposed consent agreement, it places the order on the record for public comment through the Federal Register (which is the publication used to provide notice of federal administrative actions) before determining whether to make the order final. In the event of a respondent's later breach of such order, the respondent may be liable for a civil penalty for each violation. To enforce the order and assess penalties, the FTC would bring suit against the respondent in a federal district court.

## 2011 FTC Order Against Google

On March 30, 2011, the FTC issued a complaint against Google,<sup>1</sup> charging that it used deceptive tactics and violated its own privacy promises to consumers when it launched its social network — Google Buzz — in 2010.<sup>2</sup> Google agreed to settle. After publishing the Notice of the Proposed Consent Agreement on April 5, 2011 and receiving comments from interested persons, on October 24, 2011, the FTC accepted the settlement as final and issued its order.<sup>3</sup> The order (a) barred Google from future privacy misrepresentations, (b) required a comprehensive privacy program, and (c) called for regular, independent privacy audits for the next 20 years.<sup>4</sup>

## Alleged Conduct

On February 9, 2010, Google launched its Google Buzz social network through Gmail, using the information of users who signed up for Gmail (including first and last name and email contacts) to populate its social network. This resulted in previously private information being made public in many instances. While leading users to believe that they had choice over joining the network, Google allegedly made it difficult and confusing for users to opt out of the social network and the sharing of their personal information.

At launch, Google's privacy policy stated:

*When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different*

---

<sup>1</sup> <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzcmpt.pdf>

<sup>2</sup> <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf>

<sup>3</sup> <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf>

<sup>4</sup> This was the first time (1) the FTC alleged violations of the substantive privacy requirements of the U.S.-EU Safe Harbor Framework, which provides a method for U.S. companies to transfer personal data lawfully from the European Union to the United States; and (2) an FTC consent order required a company to implement a comprehensive privacy program to protect the privacy of consumers' information.



*than the purpose for which it was collected, **then we will ask for your consent prior to such use*** (emphasis added).

The FTC alleged that Google engaged in "unfair or deceptive acts or practices, in or affecting commerce," in violation of Section 5(a) of the FTC Act by:

- ) deceiving consumers about their ability to decline enrollment in Google Buzz;
- ) failing to adequately disclose that certain information would become public by default;
- ) falsely representing to users signing up for Gmail as to its use of their information;
- ) falsely representing that it would seek users' consent before using their information for a purpose other than that for which it was collected; and
- ) misrepresenting its compliance with the U.S.-EU Safe Harbor Framework due to its failures in giving consumer notice and choice.

### The Consent Order

On October 24, 2011, the FTC accepted the proposed settlement and issued an order, set to terminate on October 13, 2031 with certain exceptions, requiring Google to, among other things:

- ) Stop misrepresenting the privacy and confidentiality of any "covered information"<sup>5</sup> and Google's compliance with any privacy, security, or other compliance program;
- ) Provide users a clear and prominent notice and obtain express affirmative consent prior to sharing Google users' information with any third party if contrary to stated practices;
- ) Establish and maintain a comprehensive privacy program to (1) address privacy risks for new products and services, and (2) protect the privacy of covered information;
- ) Obtain within 180 days, and on a biennial basis thereafter for twenty (20) years, an assessment and report from a third-party auditor certifying the program's adequacy; and
- ) Retain certain records.

### 2012 EPIC Suit

In 2012, EPIC filed a lawsuit in federal court to compel the FTC to enforce the 2011 Google consent order after Google changed its terms of service for over 60 major products.<sup>6</sup> The terms announced that Google would consolidate user data across services, creating a single merged user profile. The court dismissed the complaint over lack of jurisdiction, noting that "the FTC's decision whether to take action with respect to a potential violation of the Consent Order is a quintessential

---

<sup>5</sup> "Covered information" is defined broadly to include an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.

<sup>6</sup> <https://epic.org/privacy/ftc/google/consent-order.html>



enforcement decision that is committed to the agency's discretion and is not subject to judicial review."<sup>7</sup> The court acknowledged, however, that EPIC and others advanced "serious concerns" with respect to Google's changes.<sup>8</sup> The US Court of Appeals for the D.C. Circuit affirmed the lower court's ruling.<sup>9</sup>

---

<sup>7</sup> *Elec. Privacy Info. Ctr. v. F.T.C.*, 844 F.Supp.2d 98 at 106 (D.D.C. 2012), available at <https://epic.org/privacy/ftc/google/EPICvFTC-CtMemo.pdf>.

<sup>8</sup> *Id.*.

<sup>9</sup> *Elec. Privacy Info. Ctr. v. F.T.C.*, No. 12-5054, 2012 WL 1155661 (D.C. Cir. Mar. 5, 2012).

## Attachment C: Google's advertising contract terms

### A. Lack of transparency, requirement to comply with a broad range of policies and ability for Google to unilaterally vary

Examples of the clauses that are not transparent, that specify that Google's customers are required to comply with a broad range of policies and that provide Google with a unilateral right to vary those terms are:

1. **Google Advertising Program Terms:** *"Program Use is subject to applicable Google policies available at [google.com/ads/policies](https://support.google.com/adspolicy/answer/6020954?hl=en&ref_topic=1626336), and all other policies made available by Google to Customer, including Partner policies, and to the extent applicable, the Google EU User Consent Policy at [privacy.google.com/businesses/userconsentpolicy](https://support.google.com/adspolicy/answer/6020954?hl=en&ref_topic=1626336) (in each case, as modified from time to time, "Policies")."*<sup>1</sup> (Part of clause 2.)

Note that the link "[google.com/ads/policies](https://support.google.com/adspolicy/answer/6020954?hl=en&ref_topic=1626336)" contains links to 23 separate policies, many of which are lengthy and contain links to even further documents, for example: [https://support.google.com/adspolicy/answer/6020954?hl=en&ref\\_topic=1626336](https://support.google.com/adspolicy/answer/6020954?hl=en&ref_topic=1626336). This is even before consideration is given to what is covered by "and all other policies made available by Google to Customer". And of course in each case the relevant small business is required to comply with all of these myriad of policies as they may be "modified from time to time".

2. **AdSense Program policies:** *"All publishers are required to adhere to the following policies, so please read them carefully. ... Because we may change our policies at any time, please check here often for updates. In accordance with our online Terms and Conditions, it's your responsibility to keep up to date with, and adhere to, the policies posted here."*<sup>2</sup> (See opening paragraphs.)

Note that this page has 17 different policy "groupings", in many cases referring publishers to other pages of the Google site with multiple other policies.

3. **AdMob Advertiser Guidelines and Policies:** *"These guidelines are a general statement of AdMob's advertising standards and are not intended to be comprehensive. Third-party advertising is subject to internal review by AdMob. Adherence to the guidelines outlined below does not guarantee AdMob's acceptance of advertising content, and is not necessarily sufficient to meet the standards of all applicable laws."*<sup>3</sup> (See opening paragraphs.)

Note that this page refers to the "Google Ads advertising policies" (see paragraph A.1 above), AdMob's content policies, applicable to "(a)ds that are part of the exchange or created using the house ads tools" (with the link taking the reader to a separate page that has 27 policies – see [https://support.google.com/admob/answer/6128543?hl=en&ref\\_topic=2745287](https://support.google.com/admob/answer/6128543?hl=en&ref_topic=2745287) (Extra Page)) and, for AdMob reservation ads, an additional 19 policies at separate links.

---

<sup>1</sup> [https://payments.google.com/payments/apis-secure/get\\_legal\\_document?ldi=30847](https://payments.google.com/payments/apis-secure/get_legal_document?ldi=30847), Section 2 (Policies).

<sup>2</sup> <https://support.google.com/admob/answer/48182?>

<sup>3</sup> [Advertiser Guidelines and Policies](https://support.google.com/admob/answer/48182?)

## B. Google's unfettered rights to remove ads

**Google Advertising Program Terms (part clause 1):** "Google and its affiliates or Partners may reject or remove a specific Target, Ad, or Destination at any time for any or no reason."<sup>4</sup>

## C. Google's unfettered rights to terminate or suspend advertisers

1. **AdMob & AdSense policies:** "If you fail to comply with these policies without permission from Google, we reserve the right to disable ad serving to your app and/or disable your AdMob account at any time. If your account is disabled, you will not be eligible for further participation in the AdSense and/or AdMob program(s)."<sup>5</sup> (Part opening paragraph.)

Note that the "these policies" that are referred to in the above extract are the Extra Page policies referred to in paragraph A.3 above.

2. **AdMob Invalid activity: Disabled account policy:** "Lastly, Google does reserve the right to disable an account for any reason, including invalid activity from any source."<sup>6</sup> (Last paragraph of answer to "My account was disabled and my appeal was denied. Is there any way I can rejoin the program? Can I open a new account?".)
3. **AdMob policy violation: Disabled app(s) or account policy:** "The AdMob Policy team reserves the right to disable ad serving to your app(s) and/or disable your AdMob account at any time. If your account is disabled, you will not be eligible for further participation in the AdSense and/or AdMob program(s)."<sup>7</sup> (Part of opening paragraph.)

## D. Very limited rights to appeal or dispute Google's decisions

1. **AdSense account disabled for policy reasons:** "... our decisions are typically final. ... If you feel that this decision was made in error, and if you can maintain in good faith that the policy violations accrued were not due to the actions or negligence of you or those for whom you are responsible, you may appeal the disabling of your account. ... We will review your request as soon as one of our specialists is available. However, please keep in mind that we reserve the right to disable an account for violations of program policies, and there is no guarantee that your account will be reinstated. Please note that due to the volume of appeals we receive, you may only submit two appeals in any given month. Any additional submissions within a 30 day period will not be reviewed."<sup>8</sup> (Part answer to question "Can my account be reinstated after being disabled for policy reasons?".)
2. **AdMob Invalid activity: Suspended account:** "If we determine that your account has invalid traffic, then we may suspend your account and refund all account earnings along with Google's revenue share to impacted advertisers. ... Suspensions are non-appealable."<sup>9</sup> (Opening 2 paragraphs.)

---

<sup>4</sup> [https://payments.google.com/payments/apis-secure/get\\_legal\\_document?ldi=30847](https://payments.google.com/payments/apis-secure/get_legal_document?ldi=30847)

<sup>5</sup> [https://support.google.com/admob/answer/6128543?hl=en&ref\\_topic=2745287](https://support.google.com/admob/answer/6128543?hl=en&ref_topic=2745287)

<sup>6</sup> <https://support.google.com/admob/answer/6197403>

<sup>7</sup> [https://support.google.com/admob/answer/6195033?hl=en&ref\\_topic=2745287](https://support.google.com/admob/answer/6195033?hl=en&ref_topic=2745287)

<sup>8</sup> <https://support.google.com/adsense/answer/2576043>

<sup>9</sup> <https://support.google.com/admob/answer/6213019>