COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

Dutch Data Protection Authority

Investigation into the combining of personal data by Google

Report of Definitive Findings

November 2013
z2013-00194

PUBLIC VERSION
No rights can be derived from this informal English translation

TABLE OF CONTENTS

SUMMARY

The Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens] has launched an investigation into the combining of personal data by Google since the introduction of its new privacy policy on 1 March 2012.

Google was founded on 4 September 1998 and has its head office in California, USA. Its stated mission is: '*to organize all the world's information and make it universally accessible and useful'*. For this purpose Google not only offers an internet search engine (hereinafter called 'Search'), but it also provides a large portfolio of online services ranging from webmail (Gmail), selling online advertising (DoubleClick) and online maps (Maps) to a video service (YouTube) and a browser (Chrome).

Virtually all the services Google provides are free to the end-user. Google's business model is based on advertising revenues. Google reaches almost every person in the Netherlands with internet access via its services. Search has a usage share of more than 90% in the Netherlands. Google also uses cookies and scripts to read information from users' devices. More than 20% of the most visited websites in the Netherlands contain DoubleClick advertisements and more than 65% contain Analytics code. Visitors to these websites therefore encounter one or more Google cookies. Google's mobile operating system, Android, had a 69% usage share in the Netherlands at the end of the third quarter of 2013.

GPP2012

Google's new privacy policy, which was introduced on 1 March 2012, states that Google can combine data from all its services with data from other Google services (including cookies which it sets and reads via third-party websites). This report investigates four purposes for which Google combines data: the personalisation of requested services, product development, display of personalised ads, and website analytics.

The Dutch DPA distinguishes between three types of users: authenticated users (signed in with a Google account), unauthenticated users (people using services such as Search without a Google account), and passive users (people who visit third party websites with Google cookies).

Applicable law and data controller

The *Wet bescherming persoonsgegevens* (Wbp) [Dutch Data Protection Act] governs the processing of personal data by Google Inc. Google Netherlands B.V. is the establishment of Google Inc. in the Netherlands in the context of whose activities the processing of personal data is carried out (Article 4(1) of the Wbp).

Personal data

Google collects and processes personal data as defined in in Article 1(a) of the Wbp from all three types of users. In many cases Google collects these data with the aid of tracking cookies. This is governed by the legal presumption contained in Article 11.7a of the *Telecommunicatiewet* (Tw) [Telecommunications Act] that this constitutes the processing of personal data.

Purposes

Because the examined purpose specifications described in GPP2012 and Google's new stated purpose of its data processing activities, i.e. 'the provision of the Google service', are ambiguous and insufficiently specific, Google does not collect the data for specific purposes and is therefore acting in breach of the provisions of Article 7 of the Wbp. Because Google has no legal ground for processing the data for the four examined purposes, the personal data collected by Google from all three types of users are not being collected for legitimate purposes (as being examined here), with the result that Google is acting in breach of the provisions of Article 7 of the Wbp in this respect as well.

Information

Because of the lack of information on its identity as data controller on the YouTube website, the fragmented and inconsistent method of providing information and the lack of specific information about the types of personal data and the purposes for which Google combines these data, Google is acting in breach of the provisions of Articles 33 and 34 of the Wbp. Google is acting in breach of the provisions of Article 33 of the Wbp insofar as it receives the personal data directly from the data subjects (from authenticated users when they create a Google account and from unauthenticated users when they use Search or carry out an action such as uploading a video to the YouTube servers). Google is acting in breach of the provisions of Article 34 of the Wbp insofar as it receives the personal data by a means other than directly from users or data subjects (e.g. data on the use of Google services and visits to third-party websites via DoubleClick and Analytic cookies).

Legal ground

Google has stated that it has a legal ground for processing the data under Article 8, (opening words) and (a), (b), or (f) of the Wbp.

Unambiguous consent

With regard to the legal ground for consent, Google often collects personal data with the aid of tracking cookies and thereby does not meet the consent requirement in Article 11.7a of the Tw and the obligation to provide users with clear and complete information in accordance with the Wbp. This applies to both its own websites and those of third parties. Google must also have a legal ground for the examined data processing activities pursuant to Article 8 of the Wbp. In view of the similarities with Article 11.7a of the Tw, and in view of the intention of the European legislator to provide the same level of protection under both statutory standards and the overlap between the definitions of consent and unambiguous consent, it would seem logical to assume that there is a requirement for unambiguous consent for the personal data processing activities associated with the cookies (including the processing activities resulting from them).

However, there is no evidence of unambiguous consent as referred to in Article 8, opening words, and (a) of the Wbp, since Google does not offer data subjects any (prior) options to consent to or reject the examined data processing activities.

Insofar as Google claims that acceptance of its general terms of service and privacy policy amounts to consent, it is evident from the legislative history that unambiguous consent cannot be obtained through general terms of service. The legislative history also tells us that 'unambiguous' means that the data controller may not assume consent based on the failure to act or silence on the part of the data subject. However, Google assumes tacit consent and offers, at most, partial opportunities to opt out.

Finally, consent – unambiguous or otherwise – requires the information to be specific and the data subject to be informed. As shown above, Google does not adequately inform users about the fact that it combines personal data from different services, with or without the aid of cookies.

Necessary for the performance of the contract and legitimate interest
Because Google in many cases uses tracking cookies for the combining of personal data for the four examined purposes, unambiguous consent is as a rule required for the associated data processing activities. Therefore, claiming a legal ground under Article 8, opening words , (b) and (f) of the Wbp will not succeed for these reasons alone.

Google has not demonstrated and this investigation has not shown that the investigated data processing activities relating to the combining of data about and from multiple services are necessary (i.e. meet the requirements of proportionality and subsidiarity).

With regard to claiming a legal ground under Article 8, opening words, and (b) of the Wbp, there is no justification for the processing activities under investigation in its relationship with the specific individual data subjects (and any agreement entered into with them). Passive users will in most cases not even be aware that they have or will encounter Google cookies when using third-party websites. The terms of service therefore certainly do not give rise to a contractual relationship with passive users.

With regard to claiming a legal ground under Article 8, opening words, and (f) of the Wbp, Google has not argued convincingly that its legitimate interest in processing the data for the four purposes under investigation outweighs the data subject's right to the protection of their privacy. The combining of data by Google from and about multiple services and third-party websites for the purpose of displaying personalised ads, personalisation of services, product development and analytics constitutes a major intrusion into the privacy of the users involved.

Some of these data are of a sensitive nature, such as payment information, location data and information on surfing behaviour across multiple websites. What is more, Google offers highly diverse services which serve entirely different purposes from the point of view of users (browsing, email, viewing videos, consulting maps).

Because of the nature of the data, the diversity of the services, the lack of adequate and specific information and the lack of effective opt-outs, Google's legitimate interest does not outweigh the data subject's right to protection of their personal data and privacy (this applies to all three types of users).

The considerable usage share the various Google services have in the Netherlands also plays a role in assessing the impact of the data processing activities on the data subjects' privacy. In practice it is almost impossible for a Dutch internet user not to interact with Google even without opening a Google account, be it via Search, YouTube or Maps, or passively through third-party websites by way of DoubleClick and/or Analytic cookies.

In addition, Google has failed to put adequate safeguards in place to ensure that the combining of data is strictly limited to what is necessary in the context of the legitimate purposes and that the data subject's right to protection of their privacy prevails.

Alternatively to the view that when using personal data obtained with the aid of tracking cookies Google can only claim unambiguous consent as a legal ground for the resultant or associated data processing activities, the Dutch DPA concludes that Google cannot claim a legal ground under Article 8, opening words, (b) and (f) of the Wbp for the four examined forms of data processing, primarily due to the absence of necessity and secondarily, when invoking Article 8(f) of the Wbp, due to the absence of safeguards such as transparency and effective opt-outs.

With regard to all three types of users, there is no legal ground as required under Article 8 of the Wbp for the combining of data for the four actual purposes that have been examined in this report. Google does not obtain unambiguous consent for the examined data processing activities and has no other legal grounds under Article 8 of the Wbp. For this reason, by combining data from and about multiple services for the four examined actual purposes Google is acting in breach of Article 8 of the Wbp.

1. Introduction

Pursuant to Article 60 of the Wbp, the Dutch Data Protection Authority (Dutch DPA), in its official capacity, initiated an investigation into the privacy policy of Google Inc. (hereinafter called 'Google'), which was amended on 1 March 2012.

Google, which has its registered offices in California, USA, is engaged in the provision of a large number of globally accessible internet services, ranging from email to a search engine and from the provision of online advertising to a social network. On 1 March 2012, Google amended its global privacy policy. Instead of separate privacy terms and conditions for many of its services, Google is now using one overarching privacy policy. According to this policy, Google can combine data from many different services for other services. Google combines data for purposes such as product innovation, marketing/advertising and security.

Before this new privacy policy entered into force, the French data protection authority (CNIL) and the chair of the Article 29 Working Party of 27 EU data protection authorities jointly requested Google to delay its introduction until the investigation into the legitimacy of its data processing activities in Europe under the new privacy policy had been completed. Google refused to do so, claiming (briefly summarised) that the new policy contained no material changes. According to Google, all its old product terms of service already permitted the data of logged-in users to be combined.

On behalf of and at the request of the Article 29 Working Party, the CNIL initiated an investigation into the legitimacy of this situation under the EU Privacy Directive (Directive 95/46/EC). In March and May 2012 the CNIL asked Google a series of detailed questions and drew up a report in October 2012. In a letter dated 16 October the Article 29 Working Party informed Google about the conclusions of its investigation.

In brief, the CNIL concluded that Google:

1. is acting in breach of its obligation to provide information, especially in respect of 'passive' users;
2. has no legal ground for the combining of data from various services for a number of specific purposes;
3. wrongly omits to state retention periods either in its privacy policy or in its communication with the data protection authority.

During a press conference on these investigation results in Paris on 16 October 2012, the CNIL announced on behalf of the Article 29 Working Party that Google was being given three to four months to comply with the EU privacy legislation.

In a letter dated 8 January 2013, Google wrote that it intended to implement some changes as a result of the investigation. These involved (i) informing European users of Google services about the use of cookies, (ii) separately listing specific types of personal data in its privacy policy, namely location data, credit card data, unique equipment identifiers, telephone data and biometric data, and (iii) a pan-European review by Google itself of the Google Analytics contractual terms.

At Google's explicit request, the Article 29 Working Party received a delegation from the company on 19 March 2013. In a letter dated 26 March 2013, Google stated that it would carry out the three proposed changes described above between 8 April and 31 August 2013.

In response to the above, the Dutch DPA initiated an investigation on the basis of its supervisory role.

The investigation focused on the following questions:

- Are certain data which Google collects and processes personal data as defined in Article 1, opening words, and (a) of the Wbp?
- Does the new privacy policy, in combination with additional information, provide data subjects with the information referred to in Articles 33 and 34 of the Wbp?
- Does Google have a legal ground for combining (processing) data from different services as referred to in Article 8 of the Wbp?
- Are the purposes for which Google processes data (in the context of the combining of data) legitimate and specific as referred to in Article 7 of the Wbp? This relates in particular to the following purposes:
  1. the provision of services to passive users
  2. product development
  3. advertising purposes
  4. analytical purposes
- Are the personal data that Google collects and processes for the aforementioned combination purposes relevant and not excessive, as referred to in Article 11 of the Wbp?

The investigation therefore focuses on an assessment of compliance with Article 7 (explicitly defined, specific and legitimate purposes), Article 8 (legal ground for the data processing: unambiguous consent, performance of a contract or legitimate interest) in combination with Article 11.7 a of the Tw, Article 11 (relevant and not excessive), Articles 33 and 34 (obligation to provide information) and 6 of the Wbp (data processing carried out in a fair and careful manner).

2. PROCEDURE

2.1 Course of events

On 24 January 2012, Google announced via a notice on its blog that it intended to amend its privacy policy.[1] In a letter dated 2 February 2012, the Article 29 Working Party announced that it wanted to analyse the new privacy policy and asked Google to delay its introduction. In a letter dated 3 February 2012, Google refused the request, stating its reasons. On 27 February 2012, the French data protection authority, CNIL, on behalf of the Article 29 Working Party, once again asked Google to delay the

[1] Google Official Blog, 24 January 2012, URL: http://googleblog.blogspot.nl/2012/01/updating-our-privacy-policies-and-terms.html. 11 november 2013

introduction of the amended version until the investigation was completed. Google also rejected this request in a letter dated 28 February 2012.

Then in a letter dated 16 March 2012, the CNIL, on behalf of the Article 29 Working Party, asked Google a series of detailed questions about the changes in its privacy policy. In the letter Google was asked to reply by no later than 5 April 2012.

Google answered the first 24 questions in a letter dated 5 April and the remaining questions in a letter dated 20 April 2012. In a letter dated 22 May 2012, the CNIL asked for more specific answers to some of the questions and rephrased some of the questions. Google was asked to reply by no later than 8 June 2012. Google replied by letter dated 21 June 2012, in which it repeated some of its earlier answers.

In a letter dated 16 October 2012, the Article 29 Working Party informed Google about the conclusions of the investigation along with an annex containing the main results of the CNIL investigation.[2]

Google itself made the correspondence with the CNIL public, including the report referred to above.[3]

Google responded to the CNIL report by letter dated 8 January 2013.

At Google's explicit request, a delegation of the Article 29 Working Party received a delegation from the company on 19 March 2013.[4] The Article 29 Working Party delegation consisted of representatives of the Dutch DPA, the CNIL and the UK, Hamburg, Italian and Spanish data protection authorities (hereinafter called the Taskforce).

Google provided additional information in a letter dated 26 March 2013.

In a letter dated 2 April 2013, the Dutch DPA announced to Google that it intended to initiate an ex officio investigation . The same day the other members of the Taskforce also announced their own investigations under their national laws. In a letter dated 8 April 2013, the Dutch DPA promised each of the members of the Taskforce that it would cooperate in exchanging information, both in respect of the Dutch DPA's own findings and information obtained from Google, in accordance with Article 28(6) of the Privacy Directive. In the letters it was emphasised that all data must be treated as confidential. In letters dated 29 March, 12 April, 22 April, 2 and 4 April 2013, the CNIL,the UK, Hamburg, Italian and Spanish data protection authorities respectively

[2] Article 29 Working Party letter dated 16 October 2012 to Google, with annex setting out the main findings of the investigation, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_google_privacy_policy_recommendations_cnil_en.pdf.

[3] Google Europe Blog, last updated on 21 June 2012, URL: http://googlepolicyeurope.blogspot.nl/2012/02/more-information-on-our-privacy-policy.html.

[4] The CNIL sent Google an invitation to this on 28 February 2013. Google accepted the invitation by letter dated 6 March 2013.

promised that they would cooperate in the exchange of information with the Dutch DPA.

In a letter dated 9 April 2013, Google acknowledged receipt of the correspondence with the various data protection authorities. The CNIL responded to this on behalf of the Taskforce by letter dated 17 April 2013.

By letter dated 23 April 213, Google replied to the Dutch DPA's letter dated 2 April 2013.

The Dutch DPA discussed the explanation of the provisions of Article 11.7a of the Tw in the context of the Dutch DPA-OPTA cooperation protocol of 12 July 2005 with the ACM.[5] The ACM agreed with this on 19 July 2013.

The Dutch DPA finalised the Report of Preliminary Findings on 25 July 2013. In a letter dated 25 July 2013, the Dutch DPA gave Google Netherlands BV (hereinafter called Google Netherlands) the opportunity to put forward its written view on the Report of Preliminary Findings. In a letter dated 2 August 2013, Google Netherlands asked the Dutch DPA to postpone the deadline for submitting its response by four weeks until 25 September 2013. In a letter dated 6 August 2013, the Dutch DPA granted Google Netherlands a postponement until the end of business day on 19 September 2013. Google Netherlands submitted its written view on 19 September 2013.

On 25 September 2013, the Dutch DPA contacted the lawyer acting for both Google and Google Netherlands by telephone.

In a letter dated 26 September 2013, the Dutch DPA sent Google Inc. an explanation of an error in the Report of Preliminary Findings which stated Google Netherlands as the establishment was responsible for the data processing activities, and also sent Google Inc. a copy of the report. Google Inc. was invited to put forward a supplementary written view within two weeks. Google Inc. responded by letter dated 10 October 2013 stating that it had nothing further to add to Google Netherlands' written view.

The Dutch DPA again discussed the explanation of the provisions of Article 11.7a of the Tw in the Report of Definitive Findings with the ACM. The ACM agreed with it on 7 November 2013.

The Dutch DPA finalised the Report of Definitive Findings on 12 November 2013.

Where the Dutch DPA used the investigations by the CNIL and the UK, Hamburg, Italian and Spanish data protection authorities for the purpose of ascertaining facts, it verified the accuracy of the information itself. The investigation results and sources

[5] By virtue of Article 42(6) of the *Instellingswet Autoriteit Consument en Markt* (IACM) [Act establishing the ACM], the ACM took over from OPTA in this the Dutch DPA-OPTA cooperation protocol on 1 April 2013.

used are documented in the footnotes to this report and have therefore also been made transparent and accessible for Google.

2.2 Google's written view on the preliminary findings of the Dutch DPA of 25 July 2013

In its written view of 19 September 2013 on the Dutch DPA's Report of Preliminary Findings, as supplemented on 10 October 2013 (hereinafter jointly called the 'written view'), Google disputes that it has contravened the Wbp for the reasons summarised below.

First and foremost, the Wbp is not applicable to a large extent because Google does not process personal data of passive and unauthenticated users. Google states that it has refuted the legal presumption set out in Article 11.7a of the Tw in respect of tracking cookies. Google has no access to actual resources with which to directly or indirectly identify unauthenticated and passive users. The data from these two groups therefore do not constitute personal data.

Google argues that the Dutch DPA incorrectly identifies Google Netherlands as the controller of the data processing activities. The data controller is Google Inc. Google Netherlands does not supply services to which the privacy policy applies, users enter into an agreement with Google Inc., and Google Netherlands neither sets nor reads cookies. Furthermore, Google Netherlands is not the national representative of Google Inc.

Google does not agree with the identification by the Dutch DPA of the four examined purposes of the data processing activities. The purpose for which Google processes these data is to provide one integrated service. According to Google, the new privacy policy and all the other information that Google provides contain sufficient details and sufficiently specific information about the way in which Google processes the data. The policy is aimed at a very wide group of users and is not unnecessarily complicated or written in legal language. The fact that Google often uses words such as 'may' is unavoidable because the actual processing depends on several factors, such as whether the user uses a particular Google service. A privacy policy does not need to spell out what a data controller is <u>not</u> going to do and does not need to go into details about future data processing operations. In this regard Google cites the opinion of the Article 29 Working Party on purpose limitation.

With regard to cookies, Google takes the view that it is acting in accordance with the law on its own websites, for example by displaying an information bar. Google furthermore claims that the website owners who allow Google cookies to be placed and read are responsible for informing their visitors and obtaining their consent. For this purpose Google has entered into contractual arrangements with these website owners. The Analytics cookies are not tracking cookies because a different identifier is used for each website. With regard to the +1 cookies, these are not used to plot users' surfing behaviour. With regard to DoubleClick cookies, Google informs visitors about these via the info button in the advertisements displayed.

Google may appeal to several legal grounds in Article 8 of the Wbp. In many cases that will be consent, Google writes. Authenticated users consent by accepting the

terms of service and the privacy policy, and unauthenticated users consent by continuing to use the website. Google obtains consent for the use of cookies on its own websites and through the information and consent mechanisms of partners websites. With regard to users of its services, Google also believes that it can appeal to the necessity of processing data for the performance of the contract. In addition, Google can in many cases appeal to the fact that the processing activities are necessary in order to uphold its legitimate interests. In those cases, the interests and the fundamental rights and freedoms of data subjects do not prevail over the interests of Google because Google offers tools with which users can exercise their rights and because Google offers users detailed information. Under the Wbp it is not necessary to offer a general right to object to the combining of data.

The purpose for which Google processes the data (to provide the Google service) is not inadequately specified. Because Google has one or more legal grounds for its data processing activities, Google does in fact process the data for a legitimate purpose.

Finally, Google disputes the view that the combining of data amounts to excessive data processing. Google processes the information in order to be able to provide its online service to users. The Dutch DPA wrongly assumes that if the privacy policy does not explicitly exclude something, Google will or may do that in the future.

The content of Google's written view can be found in **annex I** to this report, divided up by section (entitled '**Written view from Google**'). Annex I also contains the Dutch DPA's response to it and information on whether the response resulted in amendment of the findings and any resulting amendments to the conclusions. This annex forms an integral part of this report.

3. ACTUAL FINDINGS

3.1 Description of the organisation

Google was founded on 4 September 1998 and has its head office in California, USA. Its stated mission is: '*to organize all the world's information and make it universally accessible and useful*'.[6] For this purpose Google not only offers an internet search engine (hereinafter called 'Search'), but it also provides a large portfolio of online services ranging from webmail (Gmail), selling online advertising (DoubleClick) and online maps (Maps) to a browser (Chrome).

In its terms of service, Google explains that all services are provided by Google Inc., established inMountain View, California.[7] Google provides its online services in 22 of the 23 official languages of the European Union (every one except Maltese), and Google's services are available in 25 of the 27 top-level country domains of the EU

[6] Source: Google corporate information, URL: http://www.google.nl/intl/nl/corporate/facts.html.

[7] Google terms of service (last amended on 1 March 2012), URL: https://www.google.nl/intl/en/policies/terms/regional.html (forensically recorded by the Dutch DPA on 15 July 2013). The Dutch DPA is aware that Google is updating its terms of service on 11 November 2013, but these amendments fall outside the scope of this investigation.

(every one except .mt and .cy). In addition, smartphones with the Google operating system (Android) can be purchased in virtually all member states of the EU. Virtually all the services Google provides are free to the end-user.[8] Google's business model is based on advertising revenues. These are predominantly obtained from advertisements in Search which are based purely on the search term(s) entered.[9] Expenditure in the Netherlands on personalised ads amounts to less than 5% of expenditure on online advertisements.[10]

Google has a subsidiary in the Netherlands, Google Netherlands B.V., which has its registered offices in Amsterdam and has been registered with the Chamber of Commerce under number 34198589 since 27 November 2003. The company description of Google Netherlands B.V. is: *'The conducting of an enterprise in the field of an internet search engine and the provision of services and of information and advice on searching and retrieving information on the internet, intranet and other (electronic) communication.'*[11] In its written view, Google emphasises that Google Netherlands does not offer or provide services to which the privacy policy applies and does not place or read cookies.[12]

Google reaches almost every person in the Netherlands with internet access via its services. Search has a usage share of more than 90% in the Netherlands.[13] Google also uses cookies and scripts to read information from users' devices. The Google Display network contains more than two million websites, videos and apps worldwide.[14] More than 20% of the almost 8000 most visited websites in the Netherlands contain

[8] With the exception of Google Apps and paid services directed at businesses and advertising services (which are, naturally, not free of charge to advertisers).
[9] According to the annual report of the industry organisation IAB Nederland on expenditure on online advertising in the Netherlands, 54% of advertising budgets are spent on Search ads. URL: http://www.iab.nl/wp-content/uploads/downloads/2013/03/Online-Ad-Spend-2012_nieuw.pdf. In the associated press release, IAB writes: *'Search has a constantly growing share of the total digital advertising market. In 2011 its total share was 49.6%, but by 2012 this had risen to as much as 54%. The international player Google accounts for most of the €25 million turnover in this category.'* IAB Nederland, *'Digitale advertising markt blijft groeien'*, 21 March 2013, URL: http://www.iab.nl/2013/03/21/omzetgroei-online-advertising-markt-stagneert/.
[10] In the above IAB report on online advertising expenditure in 2012, tailored ads are included in the 'other' category (15%) of the number of display ads (29.2% of total expenditure), i.e. 4.38% of total expenditure.
[11] In 2010 Google Netherlands B.V. was appointed as the representative of Google Inc. in relation to its Street View service. See also: the Dutch DPA z2010-00582, Definitive findings of the investigation by the Dutch DPA into the collection of WiFi data with Street View cars by Google, 27 December 2010, p. 26-27, URL: http://www.cbpweb.nl/downloads_rapporten/rap_2011_google.pdf.
[12] Google's written view, paragraphs 8 and 9.
[13] Search had a 93% usage share in the Netherlands (based on qualitative research) or 94.3% (based on quantitative research) in 2012. Source: Blog by Eduard Blacquière, 8 February 2013, URL: Http://www.edwords.nl/2013/02/08/marktaandeel-zoekmachines-nederland-2012/ (forensically recorded by the Dutch DPA on 15 July 2013).
[14] *'The Google Display Network includes over 2 million sites that reach 90% of the world's online audience.'* URL: http://www.google.ca/think/products/google-display-network.html (URL last visited on 23 October 2013).

DoubleClick advertisements and more than 65% contain Analytics code. So visitors to these websites will encounter one or more Google cookies.[15]

Android, Google's mobile operating system, had a 69% usage share in the Netherlands at the end of the third quarter of 2013.[16] Android devices cannot actually be used without a Google account.[17] In its written view, Google states that users and original equipment manufacturers (of smart phones with the Android operating system) can easily switch to alternatives at low (or even no) cost and that the shares cited by the Dutch DPA are therefore not a useful measure of Google's position in these two areas. In addition, it states that the usage share given for Search is incorrect because it does not include vertical search engines, social networks and information sites such as Wikipedia.[18]

3.2 Amendment of the privacy policy

In late January 2012, Google announced by means of a notice on its official blog that it would be amending its privacy policy.[19] Google writes: *'While we've had to keep a handful of separate privacy notices for legal and other reasons, we're consolidating more than 60 into our main Privacy Policy.* (…) *What does this mean in practice? The main change is for users with Google Accounts. Our new Privacy Policy makes clear that, if you're signed in, we may combine information you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience.'*[20]

According to the (public) replies which Google gave on 30 January 2012 to questions from members of the US congress, the amendment of the privacy policy was mainly intended to enable YouTube and Search information to be shared and was therefore primarily aimed at authenticated (signed-in) users.[21] Before the amendment, these

[15] As recorded by the Dutch DPA in a crawl on 22 April 2013. This delivered the following percentages: Doubleclick.net on 1,712 of the 7,965 sites (21.5%), Google-analytics.com on 5,205 of the 7,965 sites (65.3%). The figures are similar to those obtained in a previous crawl performed in late November 2012. The crawl covered 8,472 .nl websites on the Alexa list of most visited websites in the Netherlands.

[16] Source: Marketingfacts, *'Bijna driekwart van de Nederlanders bezit smartphone'*, 22 October 2013, URL: http://www.marketingfacts.nl/berichten/bijna-driekwart-van-de-nederlanders-bezit-smartphone/ (URL last visited on 1 November 2013). In early 2013 this share was 60%. Source: Telecompaper, *Android groeit tot 60% marktaandeel in Nederland*', 20 February 2013, URL: http://www.telecompaper.com/nieuws/android-groeit-tot-60-marktaandeel-in-nederland--925992.

[17] Although it is theoretically possible to use an Android device without signing up for a Google account, the user will not be able to use the functionality of the pre-installed Google apps or download and install other apps via the Google Play app store.

[18] Google's written view, paragraph 27, footnote 1.

[19] Google Official Blog, 24 January 2012, URL: http://googleblog.blogspot.nl/2012/01/updating-our-privacy-policies-and-terms.html.

[20] Idem.

[21] *'The main change in the updated privacy policy is for users signed into Google Accounts.'* Letter from Google to members of the US Congress on 30 January 2012, URL: https://docs.google.com/file/d/0BwxyRPFduTN2NTZhNDlkZDgtMmM3MC00Yjc0LTg4YTMtYTM3NDkxZTE2OWRi/edit?hl=en_US&pli=1 (forensically recorded by the Dutch DPA on 15 July 2013). See also in the same letter: *'We had not updated YouTube's original*

data could not be used for other services. In its old Web History Privacy Notice, Google declared that search history could only be used '*to give you a more personalised search experience*'.[22]

Google implemented the announced amendment of its privacy policy on 1 March 2012. Instead of separate privacy terms for many of its services, Google now uses one overarching privacy policy, hereinafter called GPP2012 (in this report, 'GPP2012' and Google's 'privacy policy' are also understood to mean the versions as amended on27 July 2012 and 24 June 2013).[23]

From this policy it is clear that Google can combine data from a number of services for other services, for purposes such as product innovation and marketing/advertising and for analytic and security purposes. In addition to GPP2012 there are four separate product-specific privacy terms, for the Google Wallet, Google Books, Chrome and Fiber services.[24]

In reply to a question from the CNIL, Google declared that GPP2012 takes precedence over the provisions of its Terms of Service: '*Terms of Service are not meant to negate the practices outlined in the Privacy Policy.*'[25]

3.3 Combining of data

In response to the first questions from CNIL, Google writes that it can combine data provided by a user in one service with information from other services.[26] In its written view Google explains that the use of the words 'can' and 'may' in the privacy policy is in most cases explained by the fact that Google will not necessarily collect this information in all cases. Such collection depends on (i) whether the user is using a particular Google service, (ii) the relevance of the data for the specific service and (iii) whether the data are provided to Google.[27] Examples of the combining of data cited by Google are the use by advertising services of information from all other services for

---

privacy policy to include Google, with the result that Google could share information with YouTube, but not vice versa.' In its letter dated 20 April 2012, Google writes to the CNIL (unnumbered, counted page no. 3): *'The main change is for users with Google Accounts. The updated Privacy Policy makes clear that, if a user is signed in, Google may combine information a user provided from one service with information from other services. In short, we can treat the user as a single user across all of our products.'*

[22] Letter from Google to members of the US Congress.

[23] Google Privacy Policy GPP2012, URL: http://www.google.nl/intl/nl/policies/privacy/(last amended on 24 June 2013, forensically recorded by the Dutch DPA on 1 July 2013).

[24] Letter from Google to members of the US Congress, answer to question 10. Google added Fiber to the Dutch language GPP2012 of 24 June 2013 as a fourth service (with specific product policy rules), so it falls within the scope of this investigation.

[25] Letter from Google dated 21 June 2012 to the CNIL, answer to question 27.

[26] Letter from Google dated 20 April 2012 to the CNIL, answer to question 30: *'Google may combine information a user provided from one service with information from other services.'*

[27] Google's written view, paragraph 38.

the purpose of personalising advertisements[28] and the displaying of Google contact details in the Google Calendar for the purpose of organising a meeting.[29]

TABLE 1 COMBINING OF DATA BY USER TYPE

	Examples	Authenti-cated (active) users	Unauthenti-cated (active) users	Passive users
Google account	Gmail, Google+, Drive, Google Play (app store)	X		
'Open' services	Maps, Search, YouTube, Chrome	X	X	
Google services via third-party websites	Advertisements (including DoubleClick), Analytics	X	X	X

Users of Google services can be subdivided into three (dynamic) groups:

- **Authenticated (active) users** (of services such as Gmail, Google Play, Drive[30] and Google+). To be able to use these services, the user has to open a Google account and sign in (authenticate) with it.[31] When a user registers for a Google account he is asked to provide his name, e-mail address, date of birth, sex and mobile telephone number. Only the name and e-mail address are required information. Google repeatedly asks users who have not provided a mobile phone number to do so. Google permits the use of pseudonyms on Google+, but according to GPP2012 Google checks whether a user is consistently using the same name and reserves the right to change the name to the name it believes is the current name on the basis of accounts setup previously.[32]

[28] *'We also use the data we collect from all our services (...) to deliver personalised content to you, such as more relevant (...) advertisements'* [underlining added by the Dutch DPA]. Source: GPP2012.

[29] Letter from Google to members of the US Congress, answer to question 4a: *'For many years, as permitted by our privacy policies, we have combined data within individual accounts in ways that make the user experience better, for example by having a single address book shared between services like Gmail and Google Calendar.'*

[30] Google Docs was replaced by Google Drive in April 2012.

[31] Before the amendment of the privacy policy it was still possible to set up separate accounts, e.g. for YouTube.

[32] Google+ Help Center on the Google+ names policy: *'It's best to use your first name and surname because that enables you to contact the people you know and enables them to find you more easily.'* URL: https://support.google.com/plus/answer/1228271?hl=nl GPP2012: *'We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services.'* And: *'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.'*

Google also collects the unique IMEI device number of authenticated users who use the Android operating system via a smart phone, along with information about the apps installed on the device (via Google Play).[33]

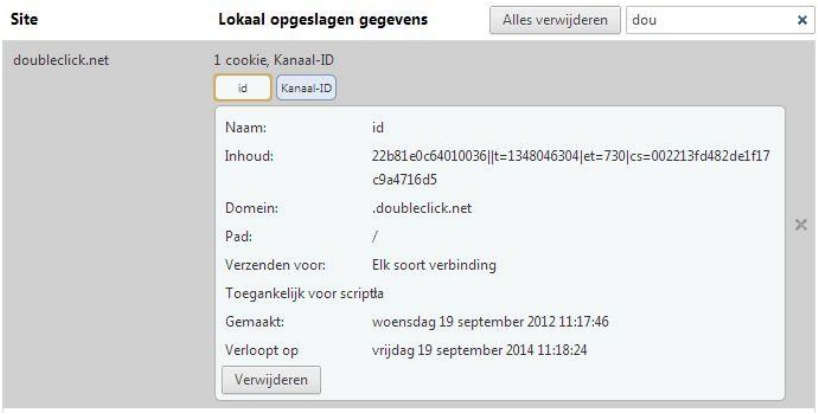
- **Unauthenticated users** (of services such as Search, Maps and YouTube). These are 'open' (freely accessible) services for which a user does not need a Google account. Users who are signed in with their Google account automatically use these services as an authenticated user, however. This group also includes holders of a Google account who opt not to sign in to 'open' Google services.[34]
- **Passive users** (who visit third-party websites that set and read Google cookies such as DoubleClick and Analytic cookies). These users are not asking Google to use its services, but Google can still process data on them via these third-party websites, such as IP addresses, cookies, browser settings and website visits (by means of URL referrers, i.e. the last website the user visited). Google also collects such data about visits to third-party websites from authenticated and unauthenticated users.

Google combines data which it obtains by and through the use of its various services by all three types of users.

- All data associated with an **authenticated user's** account may be used by any other Google service, including data from (advertisement-free) services such as Google Drive. Google uses cookies such as the APISID and PREF cookie to register use of its own services and, among other things, DoubleClick cookies to register visits to third-party websites, but it does not combine these data with directly identifiable account information (name, e-mail address and date of birth). It can not only combine authenticated users' service usage data (metadata) but also data that these users enter themselves (content data) such as the content of e-mails.
- **Unauthenticated users**' data that are collected with the PREF and Analytic cookies which Google sets on all its own websites, NID cookies used on Maps and Search and DoubleClick cookies used on YouTube, may be used by any other Google service, for example to personalise search results. In addition, DoubleClick and Analytic cookies may be used to register visits to third-party websites.
- **Passive users'** data that are collected using DoubleClick and Analytic cookies via third-party websites may be used by Google for product development, showing personalised ads and analytics purposes.

[33] The IMEI number collected and retained by Google is also visible to users when they sign in to Google, under 'Dashboard' / 'Android Devices' (forensically recorded by the Dutch DPA on 24 October 2013 via a Dutch DPA employee's Google account).
[34] The Dutch DPA notes that Google technically encourages users to remain signed in even if they switch devices and has developed Cross-Device Single Sign-on for this purpose. URL: http://googleplusplatform.blogspot.nl/2013/05/cross-platform-single-sign-on.html (URL last visited on 23 October 2013).

Example of a DoubleClick cookie



With regard to Analytics cookies, Google writes in its written view that Analytics uses a different identifier in the cookie it sets on each website and that Google Analytics does not correlate website visits between accounts of different Analytics customers. Google also points out that since May 2010 website owners have had the option to anonymise their IP address before the data are stored in the permanent memory at Google.[35] Website owners can also change a property in the Google Analytics script which will disable Analytics for every separate website visitor.[36] In addition, website visitors can install an add-on in their browser to prevent data from being sent to Google Analytics.[37]

The Dutch DPA adds that IP address anonymisation does not in fact take place because Google only removes the last octet of the IP address (in the case of current IPv4 addresses). The Article 29 Working Party wrote to Google in 2010 to point out that this method does not lead to anonymisation.[38] In addition, the fact that Google Analytics uses a different identifier on each website does not alter the fact that Google automatically collects the cookie identifier (with IP address, time, presumed location (down to city level), browser properties and URL visited[39]) when Google Analytics

[35] Google's written view, paragraph 49.
[36] Google's written view, paragraph 51.
[37] Google's written view, paragraph 50.
[38] Letter from the Article 29 Working Party to Google as search engine provider, 6 May 2010, p. 2: '*Additionally, deleting the last octet of the IP-addresses is insufficient to guarantee adequate anonymisation. Such a partial deletion does not prevent identifiability of data subjects.*' URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_05_26_letter_wp_google.pdf.
[39] '*The HTTP request for any web page contains details about the browser and the computer making the request, such as the hostname, the browser type, referrer, and language. In addition, the DOM of most browsers provides access to more detailed browser and system information, such as Java and Flash support and screen resolution. Analytics uses this information in constructing reports like the Map Overlay, Browser, and Referring Sites reports. Analytics also sets and reads first-party cookies on your visitors' browsers in order to obtain visitor session and any ad campaign information from the page request. The Google Analytics Tracking Code also reads the double-click cookie to inform Google Analytics for Display Advertisers.*' Source: Google ' How Does Google Analytics Collect Data?', URL: https://developers.google.com/analytics/resources/concepts/gaConceptsTrackingOverview?hl=en#howAnalyticsGetsData.

cookies are set and read by a website owner.[40] In addition, Google's default setting is that website owners choose to allow Google to combine Analytics Cookies with DoubleClick cookies. Website owners can also choose to use the Analytics code to collect information on the interaction of authenticated users with the +1 buttons.[41] Under the heading 'How does Google Analytics collect data?', Google writes: *'The Google Analytics Tracking Code also reads the double-click cookie to inform Google Analytics for Display Advertisers*.'[42] Google informs its customers that it uses the Analytics data it obtains in accordance with its privacy policy and that it may therefore use the data for its own purposes.[43]

The CNIL asked Google a number of specific questions about the processing of credit card data, device-specific data, telephony log data, location data and unique identifiers.[44]

In response Google declared that data from all services are used '*to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users*.' Google also listed a number of 'primary' services that use the various categories of data:

- Credit card data: Wallet, Offers, Play
- Device-specific data: '*when a user accesses a Google service from a particular device*'
- Telephony log data: Google Voice
- Location data: Maps, Latitude, location-sharing in Google+
- Unique identifiers: '*when a user accesses a Google service from a particular device, or in some cases, via a particular network (e.g. WiFi).*'[45]

Google did not provide the CNIL with an overview or a more detailed explanation of the unique identifiers or device-specific data that it processes. On 24 June 2013 Google published additional information in GPP2012 about certain identifiers and data processing activities. See also 'Measures taken' (p. 32 ff. of this report).

Google uses a number of different means/identifiers to combine data from its services as well as data it collects via third-party websites:

[40] The Dutch DPA has repeatedly ascertained (most recently on 15 August 2013) that when website owners in the Netherlands use Google Analytics a cookie is formally and technically set and read by the website owner's domain server, but that Google can only deliver the service because it simultaneously reads the cookie data (remotely). Technically, this takes place via JavaScript in the website code. The script injects a pixel into the page concerned, in which the parameters of the cookie are incorporated into the URL. At the same time as the cookie is set and read on the website's server, Google also reads its pixel with the URL with the cookie content.
[41] See, for example, the Google support page on 'Social Analytics', URL: https://support.google.com/analytics/answer/1683971?hl=nl (URL last visited on 16 October 2013).
[42] See URL: https://developers.google.com/analytics/resources/concepts/gaConceptsTrackingOverview?hl=en.
[43] Source: Google, URL: https://support.google.com/analytics/answer/3000986?hl=nl&ref_topic=2919631.
[44] List of questions by CNIL on 16 March 2012, question 6.
[45] Letter from Google of 20 April 2012 to the CNIL, answer to question 6.

1. The Google account data of an authenticated user and associated cookies relating to the userID.
2. The PREF cookie that is set and read on the user's device every time the user visits a website in the Google domain and all subdomains (including YouTube). The content of the cookie does not change if the user's status changes (regardless of whether the user is signed in or not). Google has declared that it collects general information on the use of Google services via the PREF cookie. Google states that it does not associate the unique identifier in the cookie with authenticated users' Google accounts. Google states that it uses the information, for example, to remember preferred languages and to improve spelling suggestions.[46] In its written view, Google writes that in respect of unauthenticated users, the PREF and NID cookies are used to remember the user's preferences for personalising advertisements and for reporting purposes.[47]

Example of the content of a PREF cookie[48]

PREF ID=4d57574f586*****:U=57978f90********:FF=0:LD=en:TM=136603****:LM=136688****:S=g4dDh-rY********
(domain) .google.nl (valid until) Sat, 25 Apr 2015 11:32:26 GMT (number of characters) 100

3. The DoubleClick cookies that are set and read on the devices of all types of users every time they visit a third-party website or YouTube page on which DoubleClick ads are displayed. The DoubleClick cookie is stored together with the IP address, the websites visited, ads displayed, and on mobile devices, with a device identifier (or hashed anonymous identifier[49]) and 'approximate locations'.[50]
4. The Analytics cookies (with a separate identifier for each website) that are set and read on the devices of all three types of users every time they visit a third-party website that uses the Analytics service to record user statistics.

[46] Letter from Google of 21 June 2012 to the CNIL, answer to question 12: *'The data stored in the PREF cookie is not tied to a Google account. It helps us gather general information about the use of Google services and helps improve Google services by doing things like honouring settings placed within a browser and, for example, by incorporating preferred language and improving spelling suggestions.'* In a previous reply to this question (by letter dated 20 April 2012), Google wrote: *'Yes, the use of most online Google services will result in the storage of a PREF cookie on the user's device. The PREF 'ID' is not modified when logging in and out of one or several Google accounts.* (...).'

[47] Google's written view, paragraph 57.

[48] As ascertained by the Dutch DPA on visiting www.google.nl on 25 April 2013. Part of the cookie content has been masked (replaced with asterisks) by the Dutch DPA to prevent any misuse of this identity.

[49] In its letter to the CNIL dated 21 June 2012, in reply to question 25, Google explains: '*mobile applications that use Google's AdMob advertising service hash the device identifier on the user's mobile device before sending it to Google over the network, such that Google does not receive the real device identifier. After receiving the hashed device identifier, Google takes the further step of associating the hashed device identifier with an anonymous identifier. Only the anonymous identifier is used to associate advertising-related information with a user.'*

[50] Idem.

5. Unique numbers of mobile devices instead of cookies in some mobile apps, such as IMEI, MAC address and the unique (advertising) identifiers added by the various smartphone manufacturers (or makers of the operating system).

Google claims that it has a legal ground for combining data under Article 7(a), (b) or (f) of the Privacy Directive, i.e. Article 8 (opening words) and (a), (b), or (f) of the Wbp. Google has declared: *'Google has a legitimate interest in running its business and to provide and enhance its services to its users. Google may combine data across services to create a better user experience in that context. For example, by combining data we make it easy for a signed-in user to immediately add an appointment to her Calendar when a message in Gmail looks like it's about a meeting. As a signed-in user he/she can also read a Google Docs document right in his/her Gmail, rather than having to leave Gmail to read the document.'*[51]

In its written view, Google adds that in many cases it may appeal to multiple legal grounds.[52] Google states that it can appeal to consent[53] and performance of a contract[54] in the case of authenticated users and unauthenticated users, and in respect of all groups of users, in many cases to the upholding of its legitimate interests.[55] This written view of Google is also reproduced and discussed in the evaluation of the legal ground in paragraph 4.6 of this report.

3.3.1 Cookies on Google's own websites

In its written view, Google declares that with regard to its own websites it acts in accordance with the principles anchored in the Tw, e.g. by displaying a notification bar for Dutch users on www.google.com and www.youtube.com with the text: '*Cookies help us deliver our services. By using our services, you agree to our use of cookies. OK/More information.'* The words 'More information' take the user to information about the various types of cookies used by Google and about how cookies can be managed via browser settings.[56]

In response to Google's written view, the Dutch DPA conducted an additional technical investigation into the issue of whether Google is obtaining consent in accordance with the provisions of Article 11.7a of the Tw for the setting and reading of permanent cookies with unique identifiers on its own websites.

The Dutch DPA has ascertained that when authenticated and unauthenticated users visit the most widely used Google services (www.google.nl, maps.google.nl and www.youtube.nl), Google automatically places and/or reads multiple permanent cookies with unique identifiers when the home pages are loaded.[57] For authenticated

[51] Letter from Google to the CNIL dated 20 June 2012, answer to question 34.
[52] Google's written view, paragraph 58.
[53] Google's written view, paragraphs 59-63.
[54] Google's written view, paragraphs 64-66.
[55] Google's written view, paragraphs 67-77.
[56] Google's written view, paragraph 43.
[57] Technical investigation by the Dutch DPA on 17 October 2013 into the cookies that are set and read on www.google.nl, maps.google.nl and www.youtube.nl and at what point the cookies are set. The Dutch DPA used the Google account of one of its employees to

users this concerns two NID cookies (of the .nl and .com domains) on all three websites, each with the same unique identifier. In the case of Search and Maps, a PREF cookie (with a unique identifier) is also set on the homepage, and in the case of YouTube three permanent DoubleClick cookies with a unique identifier are set on the home page.

For unauthenticated users, Google sets a PREF cookie in the visitor's browser on all three sites. On Search and Maps, a NID cookie is also added (from the .nl domain). On YouTube two permanent DoubleClick cookies are set with a unique identifier.

When an authenticated or unauthenticated user clicks on 'More information' in the information banner about cookies on Search, Google sets several permanent and session-related Analytics cookies. With unauthenticated users, a PREF cookie is also set from the YouTube domain at the same time.

This means that Google sets and/or reads these cookies before a user has been given the option to consent to the setting and reading of the cookies or has had a chance to change their browser settings or leave the site.

3.3.2 Cookies via third-party websites

In its written view, Google declares that with regard to Google cookies set via third-party websites, Google has contractual arrangements with website providers that they will provide information and obtain consent where necessary.[58]

Prompted by Google's written view, the Dutch DPA conducted an additional technical investigation into the issue of whether website owners in the Netherlands are asking passive users for unambiguous consent on behalf of Google for Google to combine personal data on their surfing behaviour on multiple websites for the four examined data-processing purposes. The Dutch DPA paid particular attention to the setting and reading of DoubleClick and Analytics Cookies on the 50 most visited websites in the Netherlands (in the .nl domain).[59]

The Dutch DPA ascertained that of the 50 most visited Dutch websites, Analytics cookies are set and read on 72% and DoubleClick cookies on 68%. Of the 34 websites that set and read DoubleClick cookies, 74% (25 websites) do not ask for prior consent

---

ascertain which cookies Google sets and reads on these websites when used by authenticated users.

[58] Google's written view, paragraph 45.

[59] Technical investigation by the Dutch DPA on 17 October 2013 based on ranking data of websites in the Netherlands on www.alexa.com, looking exclusively at .nl domain websites. Each website was loaded a maximum of 7 times, waiting 7 seconds between each loading to allow for the variation in ads offered via real-time bidding. All cookies were deleted between each visit. On each website it was ascertained whether and how the website asks for consent for the setting and reading of cookies, whether cookies are set and read before the visitor has had the opportunity to opt out, whether the consent question contains information on the setting and reading of cookies by Google, and if so, whether the consent question contains specific information on the four examined purposes for the combining of personal data by Google.

before setting and reading the cookies. Of the 36 websites that set and read Analytics cookies, 69% (25 websites) do not ask for prior consent before setting and reading the cookies. Therefore, most of the 50 most visited websites in the Netherlands that were investigated set and read DoubleClick and Analytics cookies before the user is given the opportunity to opt out. Thirty-three of the 50 websites (66%) contain some information to the effect that cookies are set and read, but none of the investigated websites that actually set Google cookies asks for unambiguous consent on behalf of Google to allow for the combining of personal data for the purposes examined in this report.

3.4 Purposes

From the privacy policy revised on 1 March 2012 and the amended versions of 27 July 2012 and 24 June 2013 (GPP2012), it is evident that Google may combine data from certain services with data from other services.

'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.'[60]

Google understands personal data as follows: *'This is 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.'*[61]

Data are combined for various purposes: *'We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you personalised content – like giving you more relevant search results and ads.'*[62]

In its report, the CNIL identifies eight different purposes for the combining of data from different services by Google:

1. The provision of services in which data are combined at the user's request (such as Contacts and Gmail);
2. The provision of services requested by the user in which data are combined without the user needing to know that this is being done (e.g. personalising search results);
3. Security purposes;
4. Product development and marketing innovation purposes;
5. The provision of the Google Account;
6. Advertising purposes, for which data from advertisement-free services such as Google Drive are also used;
7. Website analytics;

[60] GPP2012, last updated on 24 June 2013, URL: http://www.google.com/intl/nl_ALL/policies/privacy/.
[61] Hyperlink from GPP2012, URL: https://www.google.nl/intl/nl/policies/privacy/key-terms/#toc-terms-personal-info.
[62] GPP2012, last updated on 24 June 2013.

8. Academic research purposes.

Following the investigation by the CNIL on behalf of the Article 29 Working Party, the scope of the present investigation by the Dutch DPA was limited to the combining of data for purposes 2 (personalisation of requested services), 4 (product development), 6 (personalised ads) and 7 (website analytics).

Within these four purposes, the investigation looked at the combining of data about and from multiple services. 'Product development' is not understood to mean the processing of data obtained from the Search service for optimising the search engine functionality but the combining of data from multiple services to develop entirely new products.

In its written view on the Report of Preliminary Findings, Google disagrees with this categorisation into different purposes. *'This categorisation ignores Google's sole, primary objective in using personal data: to provide its online service to its users.'*[63]

3.5 Information on the combining of data

On 24 January 2012 Google began notifying the amendments to its privacy policy as of 1 March 2012 via a banner/pop-up on the main domains www.google.com and www.google.nl (for users of the search engine) and by e-mail to all Google account holders.[64] Whether and to what extent Google also reached unauthenticated and passive users is not clear.[65]

The privacy policy is accessible via a hyperlink to 'Privacy and Terms' on most Google web pages and subdomains, generally at bottom right of the screen. Clicking on this takes the user to an overview page entitled 'Google Policies and Principles'. Most of this page is dedicated to information on security measures and interaction with Google services. The privacy policy can be found on the right of the screen under the heading 'Our legal policies', below a hyperlink to the terms of service. The list of FAQs under this subheading contains a hyperlink to the general 'Good to know' pages and not to the privacy policy. The 'Good to know' pages contain guides to help end-users improve their online security. The FAQ page contains no further explanation of references to Google's privacy policy or questions about it. Under the heading 'Our legal policies' (bottom right of the screen), a heading entitled 'Some technical details' was added at the end of June 2013, with a hyperlink to a new 'Technologies and

[63] Google's written view, paragraph 24. See also paragraphs 23, 79 and 85.

[64] Letter from Google to members of the US Congress: *'On January 24, 2012, we began notifying users including those who use our products without Google Accounts, about the changes. (…) Our notification methods include emails to our users; a promotion on Google.com; in-product notices on properties such as Google Maps, Google News, YouTube and mobile search; a New icon beside the Privacy link on many Google pages; an interstitial when users sign into their Google Accounts both on computers and mobile devices; an updated website, www.google.com/policies, that explains the changes and the benefits to users; and a post on the Official Google Blog.'*

[65] Google did not answer the CNIL's questions (questions 3 a-c) on the number of people it reached with this information campaign, despite repeated requests by the CNIL. On 21 June 2012, Google wrote to the CNIL: '(…) *it's important to note that we provide many different mechanisms for users to obtain relevant privacy information about our services, in particular through our vast array of in-product privacy notices. (…) We therefore do not see how this information in isolation is helpful.*'

principles' overview page. On this page there are six specific explanations on 'Advertising', 'How Google uses cookies', 'How Google uses pattern recognition', 'Types of location data used by Google', 'How Google Wallet uses credit card numbers' and 'How Google Voice works'.[66]

Google not only informs users about its data processing activities via GPP2012 but also via separate in-product notices for a number of services. Google has declared that its privacy policy in combination with the in-product notices contains all relevant information about the data Google collects and processes within its services.[67]

In addition, Google also provides information via targeted FAQs, pages on its help portal and via official announcements on the Google blog. In GPP2012 and new notices, Google does not draw attention to the existence of this supplementary information.

GPP2012 (as last amended on 24 June 2013) contains the following information on the combining of data:

'Google may associate your device identifiers or phone number with your Google Account.'

'We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. When showing you personalised ads, we will not associate a cookie or anonymous identifier with sensitive categories, such as those based on race, religion, sexual orientation or health.

'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.'[68]

In GPP2012 Google declares the following with regard to the area of application: *'Our Privacy Policy applies to all of the services offered by Google Inc. and its affiliates, including services offered on other sites (such as our advertising services), but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.'*

Under the heading 'Specific product practices', GPP2012 contains a reference to four services with specific privacy practices, namely: Chrome, Books, Wallet and Fiber. Each of these four services refers back to the general Google privacy policy for information on how data are used. Therefore, data that Google collects via these four services may also be combined with data from other services.

[66] The pages referred to were forensically recorded by the Dutch DPA on 1 July 2013.
[67] Letter from Google dated 21 June 2012 to the CNIL, answer to question 7: *'the current Privacy Policy and in-product notices provide all relevant notification for information collected and used within Google services.'*
[68] GPP2012, last updated on 24 June 2013, URL: http://www.google.com/intl/nl_ALL/policies/privacy/.

- Chrome and Chrome OS: The Chrome product line comprises the Chrome browser, Chrome Frame and Chrome OS. The separate privacy notice begins with a link to Google's general privacy policy: *'The Google Privacy Policy describes how we treat personal information when you use Google's products and services, including when you use Chrome browser and Chrome OS to access those products and services.'*[69]
- Books: *'The main Google Privacy Policy describes how we treat personal information when you use Google's products and services, including Google Play.'* The privacy policy also states: *'All of the provisions of the Google Privacy Policy apply to books on Google Play.'*[70]
- Google Wallet: *'How we use the information we collect: In addition to the forms of use listed in the Google Privacy Policy, (...)'*[71]
- Fiber: *'How we use information we collect: The Google Privacy Policy explains how we use information we collect.'*[72]

Google has provided the CNIL with a large number of examples of what it calls 'contextual in-product notices'.[73] Six of these notices contain some information about the combining of data from different services by Google. These concern Ads (for YouTube display ads[74]), Google+[75], Offers[76], Shopping[77], Search Plus Your World[78] and Web History.[79] All other examples given by Google relate to the use of data provided knowingly to Google by authenticated users of Google services, such as documents, e-mail and the content of a personal profile on Google+, and how they can block these data against third-party use (although not against use by Google). When asked by an Article 29 Working Party delegation at the meeting on 19 March 2013, Google provided some more examples of additional information in this area in March 2013. The examples only relate to Google+ and YouTube and only cover users' options for

[69] URL: http://www.google.com/chrome/intl/nl/privacy.html (forensically recorded by the Dutch DPA on 21 March 2013).
[70] URL: http://books.google.com/intl/en-GB/googlebooks/privacy.html (in English only) (forensically recorded by the Dutch DPA on 21 March 2013).
[71] URL: http://wallet.google.com/files/privacy.html?hl=nl (forensically recorded by the Dutch DPA on 21 March 2013).
[72] URL: https://fiber.google.com/legal/privacy.html (in English only) (forensically recorded by the Dutch DPA on 21 March 2013).
[73] Letter from Google dated 21 June 2012 to the CNIL, Annex II.
[74] Idem, p. 5: *'Additionally, YouTube uses information based on the types of pages you visit on websites that are members of the Google content network.'*
[75] Idem, p. 14. On the Google+ signup page there is a checkbox that reads *'Google may use my information to personalize content and ads on non-Google web sites.*'. This is checked by default.
[76] Idem, p. 31: *'We will use information from your Google Account to personalize your experience.*'
[77] Idem, p. 39: *'Logged in users of Google Shopping will see a question mark next to 'Recently Viewed'. Clicking on this question mark triggers a pop up explaining what that means and provides a link to users to edit their view history in Web History.'*
[78] Idem, p. 42. Under the 'learn more' link, the following explanation is provided: *'Now, search gets better by including photos, posts, and more from you and your friends. When signed in with Google+, you'll find personal results and profiles of people you know or follow.'*
[79] Idem, p. 43. Under the 'Expand your web history' link, it states *'Get personalized search results and more. Web History helps deliver search results based on what you've searched for and which sites you've seen.*'

protecting content data they have uploaded themselves. The examples contain no information about how Google combines data on the use of the various services it offers.[80]

In addition, Google provides privacy information in special FAQ lists about specific services and on specific pages on each service in its Help portal. The Gmail help pages, for example, contain information on how advertisements use information in the content of e-mails.[81]

Finally, Google also provides information in its general and specific blog posts. An example of this is a posting in the Analytics blog.[82] Up until February 2013, Google also provided a separate gateway for all blog posts on privacy. The Dutch DPA has ascertained that this separate Privacy Centre has been withdrawn.[83] The Dutch DPA notes that most official Google blogs seem to be targeted at professional interested parties and not at the average user of Google services.

Main differences between present and past privacy policies

In previous versions of its privacy policy (October 2010 and November 2011), Google referred to the fact that it may combine data from different Google services. In September 2010 Google announced that it was simplifying its privacy policy and would be deleting a number of product-specific notices. It justified this with the necessity of streamlining its policy because in practice data were already shared between different services.[84]

The structure and content of the new 2012 privacy policy contain similarities with the November 2011 version.[85] Google keeps an archive with previous versions of its privacy policy. The most important difference between these two versions is the much broader scope of the new privacy policy. It replaces more than 60 product-specific privacy notices for all services except the Chrome browser and the Chrome operating system, Wallet, Books and (in the Netherlands since June 2013) Fiber. The new privacy policy does not relate to services of companies taken over by Google that have not yet been integrated.[86]

[80] Letter from Google dated 26 March 2013 to the Article 29 Working Party delegation, annex 'Samples of additional in-product notices and controls'.
[81] URL: http://support.google.com/mail/bin/answer.py?hl=en&answer =6603&topic=1668949& ctx=topic (forensically recorded by the Dutch DPA on 15 July 2013).
[82] URL: http://analytics.blogspot.nl/2012/01/googles-updated-privacy-policy-what-it.html (forensically recorded by the Dutch DPA on 15 July 2013).
[83] URL: http://www.google.com/intl/en/policies/privacy/blogs/ (forensically recorded by the Dutch DPA on 15 July 2013).The separate list of blog posts on privacy was removed in February 2013. Since then the URL has pointed to the general Google Blog, http://googleblog.blogspot.com.
[84] URL: http://googlepublicpolicy.blogspot.com/2010/09/trimming-our-privacy-policies.html (forensically recorded by the Dutch DPA on 15 July 2013).
[85] The November 2011 version contained a small number of amendments compared with the October 2010 version.
[86] In its letter to the CNIL dated 20 April 2012, Google cites a number of examples in reply to the CNIL's question 5(a), such as AdMob, Google Jobs, Location Services in FireFox and

In its written view, Google states that its privacy policy addresses an enormously wide user group spread across the whole world. Its privacy policy is therefore formulated in a way that is understandable to all users, from IT professional to grandmother.[87]

3.6 Examples of actual combining of data

'We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about.' These are the words of Google Director Eric E. Schmidt in an interview with *The Atlantic* on 1 October 2010.[88]

From the examples Google gives, it is evident that the extent to which Google actually combines data from different services depends on the context, the type of data provided by the user himself and the purpose of the data processing activities. For authenticated users (those with a Google account), according to the privacy policy all data relating to the person who set up the Google account can be combined. Google states that it only links 'personal data' of authenticated users to DoubleClick cookie data with consent, but explains that this means that it does not use the DoubleClick cookies to collect 'personally identifiable information'.[89] *'Google does not use DoubleClick advertising cookies to collect users' personally identifiable information. Google records that an ad has been presented to a browser associated with a particular cookie ID (e.g. 'abc123') and that the browser has loaded particular pages, not that a particular identifiable person has.'*[90] Google has also declared: *'DoubleClick data includes IP addresses. We do not associate original unique device identifiers.'*[91] In addition, Google has declared that it does not use 'fingerprinting' techniques (recognition of a browser by its specific settings) to personalise advertisements.[92]

Google has explained that as a result of the amendment of the privacy policy, it is able to share YouTube data with its other services and vice versa, which was not previously possible under the YouTube privacy policy.[93] This enables Google to base

---

Zagat. Google publishes no overview of services to which its privacy policy applies, only a list of its 'main consumer-facing products'. URL: www.google.com/intl/nl/about/products/index.html (forensically recorded by the Dutch DPA on 15 July 2013) On 15 July 2013 this overview contained 12 services.

[87] Google's written view, paragraph 28.

[88] URL: http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/ (URL last visited on 23 October 2013).

[89] The American expression 'personally identifiable information' relates to a limited category of data, for example in Californian data breach legislation: the full name in combination with a limited amount of other data such as social security number, driving licence, bank account number plus access code, medical information and health insurance information. Article 1798.29(2)(g) of the Californian Civil Code, which entered into force on 1 January 2012. In its explanatory notes to GPP2012, Google defines 'personal information' as information that the user provides to Google himself, *'such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google.*' See p. 22 of this report.

[90] Letter from Google to the CNIL dated 20 June 2012, answer to question 25.

[91] Letter from Google to the CNIL dated 21 June 2012, answer to the extended question 25.

[92] Idem, answer to question 54.

[93] *'We had not updated YouTube's original privacy policy to include Google, with the result that Google could share information with YouTube, but not vice versa.'* Letter from Google to members of the US Congress dated 30 January 2012.

its video recommendations partly on users' search results and vice versa, or Google can partly base the content of personalised ads which authenticated and unauthenticated users receive via third-party websites on the videos they have watched on YouTube.

On its page 'About ads in the search network, in Gmail and sites across the web'[94] (not linked from the privacy policy), Google specifically explains which sources it uses to display personalised ads to signed-in users. For ads in the search engine, Google always uses previous searches, along with 'Websites you've visited that belong to businesses that advertise with Google' and 'Previous interactions with Google's ads or advertising services'. Google explains that it uses the following data to personalise ads on third-party websites: 'Your recent geographic location', 'Types of websites and apps you visit', Websites and apps you've visited that belong to businesses that advertise with Google', 'previous interactions with Google's ads or advertising services' and 'Your Google or YouTube profile'.

Since the introduction of its new privacy policy on 1 March 2012, Google has taken over a number of companies and launched new services.
An example of a new service is Google Play Music, launched in the Netherlands on 1 October 2013, a paid service for listening to music. The service provides personal music recommendations.[95] Journalists asked whether Google '*links the data that Google collects with the music service to everything Google knows about us already*'. Google's Director of Music, Sami Valkonen, stated that Google wanted to be as relevant as possible and concurred: '*So we use what we can.*'[96] Because the Google Play terms of service apply to Google Music, it is covered by Google's general privacy policy.[97] Google has not provided users of Google Play Music with separate information, nor has it informed them whether and how any data already collected would be combined with data about and from the new service.

Another example of a new service is 'Shared Endorsements' for Google+ users, which enables Google to use Google+ users' profile photos and names in adverts for products or services they have rated with +1. On 11 October 2013 Google announced that it would be amending its terms of service as of 11 November 2013 for this purpose.[98] The summary accompanying the amendments[99] states that *'your profile name and photo might appear in Google products (including in reviews, advertising and other commercial contexts)'*. Google writes: *'When it comes to shared endorsements in ads, you can control the use of your profile name and photo via the Shared Endorsements setting. If you turn the setting to 'off,' your Profile name and photo will not show up on that ad for your favourite bakery or*

[94] URL: https://support.google.com/ads/answer/1634057?hl=nl&ref_topic=2971788.
[95] URL: https://play.google.com/about/music/.
[96] NRC Handelsblad, *Nieuwe muziekdienst van Google weet wat uw smaak is*, 3 October 2013.
[97] Google Play terms of service, URL: https://play.google.com/about/play-terms.html (URL last visited on 15 October 2013).
[98] By means of an information box on pages such as www.google.nl and on the 'Policies and Principles' page.
[99] URL: http://www.google.com/intl/nl/policies/terms/changes/.

any other ads. This setting only applies to use in ads, and doesn't change whether your Profile name or photo may be used in other places such as Google Play.'[100]

From the information provided by Google on this aspect on its support pages it is evident that users cannot opt out of the use of their profile name and/or photo in other contexts apart from advertisements, such as an app recommendation in Google Play. *'To ensure that your recommendations reach the people you care about, Google sometimes displays your reviews, recommendations and other relevant activity throughout its products and services.'*[101] In this additional information, Google actually seems to assume consent. Google writes: *'To allow people to see your name and photo in shared endorsements appearing in ads, check the box next to 'Based upon my activity, Google may show my name and profile photo in shared endorsements that appear in ads.' Then, click the 'Save' button to save your new setting.'* The Dutch DPA has ascertained that Google does not offer Dutch users an opt-in but an opt-out. The checkbox for Dutch users is checked by default.[102]

3.7 Opt out possibilities for of the combining of data

Google does not offer a general opt-out for the combining of data. However, it offers a number of partial opt-outs for three of the four examined purposes.
To the extent data are combined based on the use of cookies, Google refers to the possibility to refuse cookies in browsers, but also points out the disadvantages of doing so.[103] A large number of websites (including websites without Google cookies) often work less well when all cookies are refused.

It is not possible to object to the combining of personal data about and from multiple services for product development purposes.

With regard to the combining of personal data for website analytics, all three types of users can object to their data being disclosed to Google by installing a special plug-in (add-on) in their browser. Google offers no other ways of opting out. The ad-on must be installed separately in each browser and on each device.

Google offers the following opt-outs for the combining of data for advertising purposes. **Authenticated and unauthenticated users** can (after clicking through several times) opt out of advertisements on the sites in the Google domain via Google and can allow a separate opt-out cookie to be set for DoubleClick cookies via YouTube

[100] Idem.
[101] URL:
https://support.google.com/plus/answer/3403513?hl=nl&p=plus_sesetting&rd=1.
[102] On 24 October 2013 the Dutch DPA ascertained forensically via an employee's Dutch Google account that the checkbox referred to by Google was checked by default.
[103] Google writes: *'You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies.'*
Source: Google Policies and Principles, Key terms, Cookies, URL:
https://www.google.nl/intl/nl/policies/privacy/key-terms/#toc-terms-cookie.
11 november 2013

and third-party sites (the more than 2 million websites that form part of the Google Display network).[104]

The Dutch DPA has ascertained that a DoubleClick opt-out cookie can be set via this menu and that it is possible to instruct Google not to display any more personalised ads within its own services.[105] The DoubleClick opt-out cookie prevents the unique identifier in the cookies from being disclosed to Google via third-party websites. After a user opts out of personalised ads within Google, Google continues to read the PREF and NID cookies (with the unique identifier) on its own websites every time a user visits a page or service in the Google domain.[106]

When a user opts out from personalised ads in the Google domain and for personalised Google ads elsewhere on the Internet, a pop-up appears with the following explanation:[107]

What it means to opt out

- **You'll still see ads after opting out of interest-based advertising. The ads will be less relevant.**
- Ads won't be based on your interests and may appear in other languages.
- Your opt outs may not occur instantaneously.

Opt-out Cancel

In addition, Google describes two other opt-outs for DoubleClick cookies on this Adds Settings page, which can also be used by **passive users** of Google's services: *'You can opt out of the DoubleClick cookie, as well as other companies' cookies used for interest-based ads, by visiting the aboutads.info choices page. If you want to permanently opt out of the DoubleClick cookie, you can install the DoubleClick opt out extension.'* The page contains no specific information for users of mobile devices.

Users who use Google services actively or passively on a mobile device have to undertake additional actions to stop targeted ads from being displayed. Google describes these actions as follows[108]:

Android
Open the Google Settings app on your device.
Select Ads

[104] URL: https://www.google.com/settings/ads?hl=nl (forensically recorded by the Dutch DPA on 15 July 2013).
[105] After the user clicks on 'Opt out' for advertisements in the Google domain, a post-request is sent to Google in JavaScript but this does not lead to an opt-out cookie being set in the browser. In DoubleClick, 'Opt out' leads to a DoubleClick opt-out cookie being set. Forensically recorded by the Dutch DPA on 16 July 2013.
[106] This means that the path parameter of DoubleClick cookies after an opt-out is restricted to the page with the settings and that the unique identifier is no longer disclosed. In its letter to the CNIL dated 21 June 2012 Google comments on this as follows, in reply to question 55: *'Owing to the technical nature of the way the various opt-outs work for these services, Google may continue to collect certain data when an opt-out is exercised.'*
[107] Idem.
[108] The information has been available on the 'Advertising' information page since the end of June 2013.

iOS
Some apps on iOS 6 devices use Apple's Advertising Identifier; to learn more about limiting ad tracking using this identifier, visit the Settings menu on your iOS 6 device. Legacy apps on your iOS 6 device, as well as apps on devices running older versions of iOS, may use a different device identifier. To opt out for these apps:

Open the Google Search app on your device.
Press the Settings icon.
Go to Ads Preferences

However, disabling the unique ad identifier is not sufficient to stop personalised ads being displayed by Google. Internet users with a mobile device also have to install opt-out cookies for the various Google advertising networks such as AdMob and DoubleClick.

In response to Google's written view in which it states that it offers a range of different opt-out tools[109], the Dutch DPA conducted a more in-depth investigation into the opt-out options for the combining of data for personalisation of requested services.

With regard to the personalisation of requested services, **authenticated users** can object within each service, such as Search and YouTube, but they cannot object to Google combining data from and about their use of other services with those services, such as information on their Google+ activities (particularly results of people they know on Google+). The opt-out options Google offers authenticated users are labour-intensive[110] and have to be repeated at every visit if the history is paused or cleared. In fact, completely turning off search results does not lead to the actual clearing of search results but only prevents Google from using these data to personalise search results.[111] In addition, completely turning off search results leads to loss of functionality as authenticated users cannot search in their personal browsing history.

Unauthenticated users can also object to their web history being recorded. In the list of search results displayed, they have to click on the settings cog icon at the top right of the page (options). A drop-down menu appears with the option 'Web History'. Personalisation of search results is turned on by default, but this can be turned off. The following text appears: *'Changes based on search activity (when not logged in) are disabled.'* The text contains no hyperlinks to explanations of what this means or information

[109] Google's written view, paragraph 74.
[110] On a separate FAQ page, Google states: *'If you've disabled signed-out search history personalization, you'll need to disable it again after clearing your browser cookies. Clearing your Google cookie clears your search settings, thereby turning history-based customizations back on.'* URL: https://support.google.com/accounts/answer/54048#signedout (URL last visited on 14 October 2013).
[111] When an authenticated user deletes his search history, this does not result in Google clearing all the data, nor does it stop it from combining data from other services for this purpose or using the data for product development. Google writes in this regard: *'As is common practice in the industry, and as outlined in the Google Privacy Policy, Google maintains a separate logs system for auditing purposes and to help us improve the quality of our services for users.'* Source:
https://support.google.com/accounts/answer/54068?topic=14149&ctx=topic.
11 november 2013

about the fact that Google can still combine the data for other purposes such as product development or for showing personalised advertisements. Unauthenticated users cannot object to personalisation of results in YouTube and Maps other than by refusing all cookies in the browser (with the corresponding loss of functionality on other websites). This is because the opt-out is only available after signing in with a Google account.[112]

TABLE 2 OPTIONS FOR OPTING OUT OF THE COMBINING OF DATA PER TYPE OF USER AND EXAMINED PURPOSE

	Examples	Authenticated users	Unauthenticated users	Passive users
Personalisation of requested services	Personalisation of Search and YouTube	Partly, by service	Only of Search	N/A
Product development	All Google services	No	No	No
Advertising purposes	DoubleClick via third-party websites	No, opt-out from targeted ads only	No, opt-out from targeted ads only	No, not via Google
Website analytics	Analytics on own and third-party websites	Yes, via Google browser add-on	Yes, via Google browser add-on	Yes, via Google browser add-on

3.8 Measures taken since the start of the investigation

At the beginning of January 2013 Google announced that it intended to make some changes to its privacy policy as a result of the investigation by the CNIL on behalf of the Article 29 Working Party.[113] These involved (i) informing European users of Google services about the use of cookies, (ii) separately listing specific types of personal data in its privacy policy, namely location data, credit card data, unique equipment identifiers, telephone data and biometric data, and (iii) a pan-European review by Google itself of the Google Analytics contractual terms and conditions.

In a letter dated 26 March 2013, Google set out a concrete timetable for the intended changes referred to above.

Since mid-April 2013[114], pages of search results (web pages and images) on www.google.nl have contained a short notice on the use of cookies. The text reads as follows: *'Cookies help us deliver our services. By using our services, you agree to our use of cookies. OK/More information'* Clicking on the 'More information' button takes the user

[112] Personalisation is activated by default on YouTube. Unauthenticated users are given no option to object to this. See URL: https://support.google.com/youtube/answer/57711
[113] Letter from Google to the CNIL dated 8 January 2013.
[114] The timetable for the introduction differed between countries and user groups. The Dutch DPA forensically recorded the new banner on google.nl on 15 April 2013.

to a page with information on how Google uses cookies.[115] This page contains no way of refusing the different types of cookies via Google in one single action. It contains hyperlinks to information on the types of cookies Google may use for personalising searches and displaying personalised ads and for Google Analytics. The page also contains a hyperlink to general information explaining how users can change their cookie settings in some browsers[116] and contains specific information on how to change cookie settings in Google Chrome.

After clicking through five times, users can arrive at a menu where they can stop personalised ads from being displayed.[117] After clicking twice, at the bottom of the page, users will also find brief instructions for users of mobile devices for blocking the use by Google of 'anonymous IDs' on devices running the Android or iOS operating system for advertising purposes.

Google announced that it would provide the members of the Article 29 Working Party delegation with further information about location data, credit card data, unique equipment identifiers, biometric data and telephony on 30 June 2013.[118]

In the absence of more detailed information from Google, the Dutch DPA independently ascertained that since 24 June 2013 the 'policies and principles' page on Google's Dutch-language website has provided additional explanations about the use of identifiers in advertising, cookies, face and voice recognition (i.e. biometric data), types of location data used by Google, how Google Wallet uses credit card numbers, and how Google Voice works.

Under 'Advertising', Google explains:
Advertising keeps Google and many of the websites and services you use free of charge. (...) Many websites, such as news sites and blogs, partner with Google to show ads to their visitors. Working with our partners, we may use cookies for a number of purposes, such as to stop you seeing the same ad over and over again, to detect and stop click fraud, and to show ads that are likely to be more relevant (such as ads based on websites you have visited).'[119]

And:

[115] The link leads to the URL http://www.google.nl/intl/nl/policies/technologies/cookies/ (forensically recorded by the Dutch DPA on 15 July 2013).
[116] Google writes: *'In some browsers you can set up rules to manage cookies on a site-by-site basis, giving you more fine-grained control over your privacy. What this means is that you can disallow cookies from all sites except those that you trust.'* URL: http://www.google.com/intl/nl/policies/technologies/managing/ (forensically recorded by the Dutch DPA on 1 July 2013).
[117] By clicking on 'More information', 'How Google uses cookies', 'How Google uses cookies in advertising', 'Settings for Google ads' and 'Opt-out' (two options, one for tailored ads in Google and one for tailored ads on YouTube and the rest of the internet).
[118] Letter from Google to the CNIL dated 8 January 2013.
[119] Google Policies and Principles, 'Advertising' hyperlink, URL: http://www.google.com/intl/nl/policies/technologies/managing/ (forensically recorded by the Dutch DPA on 1 July 2013).

'To help our partners manage their advertising and websites, we offer many products, including AdSense, AdWords, Google Analytics, and a range of DoubleClick-branded services. When you visit a page that uses one of these products, either on one of Google's sites or one of our partners', various cookies may be sent to your browser.'[120]

Google explains that it not only uses cookies but also uses the IP address to determine the user's location. *'We may also select advertising based on information about your computer or device, such as your device model, browser type, or sensors in your device like the accelerometer.'* With regard to ads on mobile devices, Google writes that it uses 'anonymous IDs. *'To serve ads in services where cookie technology may not be available (for example, in mobile applications), we may use anonymous IDs. These perform similar functions to cookies.'* Google defines an 'anonymous ID' as follows: *'An anonymous id is a random string of characters that is used for the same purposes as a cookie on platforms, including certain mobile devices, where cookie technology is not available.'*[121]

The 'Advertising' page contains a hyperlink to a page with an overview of the types of cookies Google uses. On this subject, Google writes: *'Our main advertising cookie on non-Google sites is called 'id' and it is stored in browsers under the domain doubleclick.net. We use others with names such as _drt_, FLC, NID and exchange_uid.*[122]

The 'Advertising' page also contains information about opting out from advertising cookies. The page provides no explanation of the term 'partners' used on the page. The page and its sub pages contain no information about how Google combines data from different services to enable it to display more relevant ads.

Under the heading 'How Google uses cookies', Google explains:
'We use cookies for many purposes. We use them, <u>for example</u>, to remember your safe search preferences, to make the ads you see more relevant to you, to count how many visitors we receive to a page, to help you sign up for our services and to protect your data [underlining added by the Dutch DPA].'[123]

Under the heading 'Types of location data used by Google', Google describes two types of location data: 'implicit location information' and 'internet traffic information'. Google understands 'implicit location information' to mean: *'information that does not actually tell us where your device is located, but allows us to infer that you are either interested in the place or that you might be at the place.* As an example, Google cites a search for 'Eiffel Tower' from which it infers that the user is interested in Paris. It understands 'internet traffic information' to mean IP addresses and 'device-based location services' on mobile devices. On this subject, Google writes: *'these are services that use information*

[120] Idem.
[121] Google Policies and Principles, 'Key terms' hyperlink, URL: http://www.google.nl/intl/nl/policies/privacy/key-terms/#toc-terms-identifier (forensically recorded by the Dutch DPA on 15 July 2013).
[122] URL: http://www.google.com/intl/nl/policies/technologies/types/ (forensically recorded by the Dutch DPA on 1 July 2013).
[123] Google Policies and Principles, 'How Google uses cookies' hyperlink, URL: http://www.google.com/intl/nl/policies/technologies/cookies/ (forensically recorded by the Dutch DPA on 1 July 2013).

such as GPS signals, device sensors, Wi-Fi access points, and cell tower ids that can be used to derive or estimate precise location '[124]

Under the heading 'How Google Wallet users credit card numbers', Google writes: *'Google uses the credit card and debit card numbers you enter into your Google Wallet account to process payments for the online or offline purchases you make using Google Wallet, including Google Play transactions, and for fraud monitoring purposes.'* In addition, Google refers to the separate Google Wallet privacy policy. Google writes: *'We only share personal information with third parties in the circumstances described in the Wallet Privacy Notice.'*[125]

Under the heading 'How Google Voice works', Google explains: *'Google Voice stores, processes and maintains your call history (including calling party phone number, called party phone number, date, time and duration of call), voicemail greeting(s), voicemail messages, Short Message Service (SMS) messages, recorded conversations, and other data related to your account in order to provide the service to you.'*[126]

A hyperlink leading to a definition of unique device identifiers has been added to the 24 June 2013 version of the privacy policy. Google defines this term as follows:

'A unique device identifier is a string of characters that is incorporated into a device by its manufacturer and can be used to uniquely identify that device.' Different device identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed. A given device may have several different unique device identifiers. Unique device identifiers can be used for various purposes, including security and fraud detection, syncing services such as a user's email in-box, remembering the user's preferences and providing relevant advertising.'[127]

With regard to the terms of service of Google Analytics, Google declares that it already largely complies with the CNIL recommendations. Customers of the service can choose to have Google anonymise IP addresses (of visitors to their website), and there is an add-on for browsers which prevents information on visits to websites from being disclosed to Google Analytics. According to Google, the only outstanding point is its own review of its terms of service, '*which we are currently undertaking on a pan-EU level*''. Google declares that this review should be completed by 31 August 2013, at

[124] Google Policies and Principles, 'Types of location data used by Google' hyperlink, URL: http://www.google.com/intl/nl/policies/technologies/location-data/ (forensically recorded by the Dutch DPA on 1 July 2013).
[125] Google Policies and Principles, 'How Google Wallet uses credit card numbers' hyperlink, URL: http://www.google.com/intl/nl/policies/technologies/wallet/ (forensically recorded by the Dutch DPA on 1 July 2013).
[126] Google Policies and Principles, 'How Google Voice works' hyperlink, URL: http://www.google.com/intl/nl/policies/technologies/voice/ (forensically recorded by the Dutch DPA on 1 July 2013).
[127] Google Policies and Principles, 'Key terms' hyperlink, URL: http://www.google.nl/intl/nl/policies/privacy/key-terms/#toc-terms-unique-device-id (forensically recorded by the Dutch DPA on 11 July 2013).

which point it will inform the members of the taskforce what the outcomes are.[128] Since then, Google has not provided the Dutch DPA with any further details of these outcomes, neither in its written view on the Report of Preliminary Findings nor elsewhere. However, in its written view Google refers to the option for website owners to turn off Analytics for each website visitor if they want to give end-users more control before cookies are set.[129] In early October 2013 the Dutch DPA found out via the media that Google now intends to offer customers of the Analytics service in Europe a data processing contract.[130] During the investigation the Dutch DPA ascertained and verified with Google[131] that Google in the Netherlands was not offering data processing contracts to customers of Google Analytics services in the Netherlands (at least prior to 7 November 2013).

4. Assessment

4.1 Applicable law, authority and data controller

Article 4 of the Wbp stipulates:
1. This Act applies to the processing of personal data carried out in the context of the activities of an establishment of a data controller in the Netherlands.
2. This Act applies to the processing of personal data by or for a data controller that does not have an establishment in the European Union, whereby use is made of automated or non-automated means situated in the Netherlands, unless these means are used only for purposes of transit of personal data.
3. The data controller referred to under (2) is prohibited from processing personal data, unless he designates a person or body in the Netherlands to act on its behalf in accordance with the provisions of this Act. For the purposes of application of this Act and the provisions based upon it, the said person or body shall be deemed to be the data controller.[132]

Under the provisions of Article 1(d) of the Wbp, the data controller is *the natural person, legal entity or any other administrative body, which, either alone or jointly with others, determines the purpose and means of processing personal data.*[133]

[128] Letter from Google to the CNIL dated 26 March 2013, p. 1
[129] Google's written view, paragraph 51. Here Google refers to information in the Support Centre at http://www.google.nl/analytics/learn/privacy.html.
[130] URL: http://www.google.com/analytics/terms/dpa/dataprocessingamendment_20130906.html, cited in *Webwereld*, *Google past na privacydruk Analytics in heel Europa aan*, 7 October 2013, URL: http://webwereld.nl/beveiliging/79561-google-past-na-privacydruk-analytics-in-heel-europa-aan (URLs last visited on 29 October 2013).
[131] The Dutch DPA spoke to representatives of Google Netherlands B.V. about this by telephone on 11 February 2013.
[132] This article is the implementation of Article 4 of the Privacy Directive.
[133] This article is the implementation of Article 2(d) of the Privacy Directive.

According to Article 51(1) in conjunction with Article 61(1) of the Wbp, the Dutch DPA oversees '*the processing of personal data in accordance with the provisions laid down by and under the Act.*'

Under the provisions of Article 60(1) of the Wbp, the Dutch DPA, ex officio, or at the request of an interested party, can launch an investigation into the way the provisions specified in and pursuant to the law are applied to data processing.

Details of the legal framework

Applicable law

From the wording of Article 4 of the Privacy Directive, it is evident that the term 'establishment' is understood in the directive to mean one or several centres of economic activity, which may be located in various member states of the European Union.[134]

Consideration 19 of the Privacy Directive states in this regard:
Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect.

In this context, the legislative history of the Wbp informs us that in a concrete case it will need to be ascertained from the facts whether there is evidence of an establishment within the meaning of the directive and therefore whether national law applies[135]. In his advice to the European Union Court of Justice (hereinafter called CJEU) of 25 June 2013, in the matter of Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD), Advocate-General N. Jääskinen writes that he agrees with the analysis of the Article 29 Working Party in its opinion on data protection and search engines[136], namely that the business model of an internet search machine provider must be taken into account.

He writes:
'64. In my opinion the Court should approach the question of territorial applicability from the perspective of the business model of internet search engine service providers. This, as I have mentioned, normally relies on keyword advertising which is the source of income and, as such, the economic raison d'être for the provision of a free information location tool in the form of a search engine. The entity in charge of keyword advertising (called 'referencing service provider' in the Court's case-law) is linked to the internet search engine. This entity needs presence on national advertising markets. For this reason Google has established subsidiaries in many Member States which clearly constitute establishments within the meaning of Article 4(1)(a) of the Directive. It also provides national web domains such as google.es or google.fi. The activity of the search engine takes this national diversification into account in various ways relating to

[134] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 75.
[135] Idem.
[136] Article 29 Working Party, Advice 1/2008 on data protection and search engines (April 2008), p. 10-11, URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_nl.pdf.

the display of the search results because the normal financing model of keyword advertising follows the pay-per-click principle.
65. For these reasons I would adhere to the Article 29 Working Party's conclusion to the effect that the business model of an internet search engine service provider must be taken into account in the sense that its establishment plays a relevant role in the processing of personal data if it is linked to a service involved in selling targeted advertisement to inhabitants of that Member State.'
66. Moreover, even if Article 4 of the Directive is based on a single concept of controller as regards its substantive provisions, I think that for the purposes of deciding on the preliminary issue of territorial applicability, an economic operator must be considered as a single unit, and thus, at this stage of analysis, not be dissected on the basis of its individual activities relating to processing of personal data or different groups of data subjects to which its activities relate.
67. In conclusion, processing of personal data takes place within the context of a controller's establishment if that establishment acts as the bridge for the referencing service to the advertising market of that Member State, even if the technical data processing operations are situated in other Member States or third countries.[137]

Consideration 20 of the Privacy Directive states in this regard: *Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice'*

The term 'means used' in consideration 20 of the Privacy Directive implies (i) an activity practised by the data controller and (ii) the intention to process personal data.[138] The term 'means' includes human and/or technical means.[139] This also includes the collection of personal data by means of the computers of users, for example with cookies, JavaScript or banners, or by means of mobile devices of users using specific software that has been installed on the devices (such as apps).[140] The party responsible for the processing does not have to own or be in possession of the means in order for

[137] Concl. of A-G N. Jääskinen of 25 June 2013, case C-131/12 (Google Spain SL and Google Inc./Agencia Española de Protección de Datos (AEP)), URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=NL&mode=lst&dir=&occ=first&part=1&cid=417901
[138] Article 29 Working Party, Advice 8/2010 on applicable law (August 2010), p. 23 and 'Working document on the international application of the EU's data protection legislation to the processing of personal data on the Internet by websites from outside the EU' (May 2002), p. 10-11, URLs: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_nl.pdf en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_nl.pdf.
[139] For the term 'equipment' in the English-language version of the Privacy Directive, in other EU languages – such as Dutch – the word 'means' is used. This argues in favour of a broad interpretation of the term. Article 29 Working Party, Advice 8/2010 on applicable law, p. 9-10.
[140] Idem, p. 23-24. See also Article 29 Working Party 'Working document on the international application of the EU's data protection legislation on the processing of personal data on the Internet by websites outside the EU', p. 13 ff.

the processing to be within the scope of the Wbp.[141]

Jurisdiction of the Dutch DPA
Article 51(1) of the Wbp indicates that the supervisory role of the Dutch DPA is not limited to the territory of the Wbp, but also extends to other laws, general administrative regulations and other regulations on the basis of which personal data are processed.[142]

Assessment

Google does not claim that it has one or several establishment(s) in the European Union. Google writes that the services are provided by Google Inc. and not by Google Netherlands B.V.: *'Google Netherlands does not provide the services covered by the Google Inc. Privacy Policy.'*[143] Users enter into an agreement with Google Inc. Google Netherlands does not set cookies or read information from cookies.[144]

Google has had an office in the Netherlands since 2003. This office is operated by its subsidiary Google Netherlands B.V. (hereinafter called Google Netherlands). In 2011 this office had 112 employees and a turnover of €103,054,043.[145] Google has at least three data centres in the Netherlands[146] and employs engineers to maintain and develop the local infrastructure.[147]

The statutory purpose specification of Google Netherlands is: *'The conducting of an enterprise in the field of an internet search engine and the provision of services and of information and advice on searching and retrieving information on the internet, intranet and other (electronic) communication.'*[148]

[141] In the same sentence see Article 29 Working Party, Advice 8/2010 on applicable law, p. 34.
[142] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 177.
[143] Letter from Google Netherlands (in English) dated 23 April 2013, received by the Dutch DPA on 25 April 2013.
[144] Google's written view, paragraph 8.
[145] Source: Commercial Register of the Chamber of Commerce, Google Netherlands B.V., Annual Report 2011, recorded by the Dutch DPA on 26 June 2013. It is evident from the Commercial Register that Google Netherlands Holdings B.V. is also established in the Netherlands. This is a financial holding company. Google Ireland Holdings owns 100% of the shares in this holding company.
[146] Also see: URL http://www.datacenterknowledge.com/archives/2012/05/15/google-data-center-faq/ and http://www.marketingfacts.nl/berichten/20070207_google_opent_datacenter_bij_eemshaven (URLs forensically recorded by the Dutch DPA on 15 July 2013).
[147] See also the vacancies at Google in Amsterdam and Eemshaven at URL: https://www.google.com/about/jobs/search/#t=sq&q=j&jl=Amsterdam,The%20Netherlands. From these it is evident that there are engineers working in Operations and Support teams at both locations. Google in Amsterdam had a vacancy for a Network Engineer on 15 July 2013. URL: https://www.google.com/about/jobs/search/#!t=jo&jid=2868002& (forensically recorded by the Dutch DPA on 15 July 2013).
[148] Source: Commercial Register of the Chamber of Commerce, Google Netherlands B.V., recorded by the Dutch DPA on 26 June 2013.

In its 2011 annual report, Google Netherlands describes its activities as follows: '*Google Netherlands B.V. (Company) is engaged in the business of developing, licensing, marketing and selling certain Internet search, advertising and information management technology services and related products and also in the provision of research and development services (to Google Ireland Limited and Google Inc.).*'[149]

This therefore constitutes an office that effectively and actually undertakes activities for an indefinite period[150], mainly by selling advertisements to advertisers in the Netherlands, but also by developing internet, advertising and information management technology and related products and providing research and development services for the American parent company, among others.

Given the fact that Google provides virtually all of its services free of charge (with the exception of business services and a small number of services such as telephony), on the basis of the position of the A-G of the CJEU and the Advice on Data Protection and Search Machines of the Article 29 Working Party[151], in determining whether an establishment exists, the fact that Google is financially dependent on advertising revenues should be taken into account. The fact that the purpose of Google's office in the Netherlands is geared towards selling advertising on the Dutch market and the presence of a Dutch website (google.nl domain) indicate that personal data are being processed within the framework of the Dutch establishment, because this establishment functions as an essential link to the Dutch advertising market regardless of where the technical data processing activities actually take place.

Given the above, the Wbp applies to the processing of personal data by Google Inc. and Google Netherlands B.V. is the establishment of Google Inc. in the Netherlands in the context of whose activities the processing of personal data is carried out (Article 4(1) of the Wbp).

In addition, the Dutch DPA notes that the outcome of this assessment would be materially no different if Article 4(2) of the Wbp were to be applied. This paragraph stipulates that the Act is also applicable if a data controller has no establishment in the European Union but uses automated or non-automated means that are located in the Netherlands.

The Dutch DPA has established that Google uses devices (computers, mobile devices) of users in the Netherlands by setting and reading information on their devices such as cookies, unique identifiers and device settings (browser properties and OS versions) and in doing so collects IP addresses as a means of processing personal data in connection with the combining of data. Furthermore, Google uses users' smartphones to determine the geolocation of the devices based on the list of

[149] Source: Commercial Register of the Chamber of Commerce, Google Netherlands B.V., Annual Report 2011, recorded by the Dutch DPA on 26 June 2013.
[150] See also Article 29 Working Party, Advice 8/2010 on applicable law, p. 13-14.
[151] Article 29 Working Party, Advice 1/2008 on data protection and search engines , p. 11, URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_nl.pdf

surrounding Wi-Fi routers.[152] This does not concern means used solely for purposes of transit of personal data, but actual control over the personal data that is collected and processed on the devices of users in the Netherlands.

Application of this test (i.e. if there were no evidence of an establishment but evidence of the use of means in the Netherlands) would make Google Inc., of Mountain View, California, USA, the data controller for the purposes of the data processing activities, it would render the Wbp applicable and, under Article 4(3) of the Wbp, it would require it to appoint a local representative regarded by the law as the data controller for the purpose of the application of this law and the provisions based on it. In 2010 Google Inc. appointed Google Netherlands B.V. as its representative in the Netherlands, but only for the purpose of data processing in the Street View service[153]. The fact that Google Netherlands is not expressly reported as the representative of Google Inc. for services other than Street View does not alter the conclusion that Google Inc. uses means in the Netherlands for processing personal data. It follows hat, if Article 4(2) of the Wbp is declared applicable, Google Inc. must appoint a representative in the Netherlands for the data processing activities under investigation (and it has not done so).

Given the above, the Wbp is applicable to the processing of personal data by Google and the Dutch DPA, in its capacity as the supervisory authority, has jurisdiction over the processing of personal data by Google.

4.2 Personal data

According to Article 1, opening words and (a) of the Wbp, 'personal data' is defined as *all information relating to an identified or identifiable natural person*.
The 'processing of personal data' is defined in Article 1, opening words and (b) of the Wbp and includes the collecting, recording, storing, using, aligning and combining of personal data.[154]
Article 11.7a, first paragraph, second sentence, of the Tw stipulates that the placement or reading of data in the end user's terminalequipment for the purpose of collecting, combining or analysing data on the user's or subscriber's use of various information society services for commercial, charitable or ideological purposes (in other words, the use of tracking cookies) is presumed to constitute data processing as referred to in Article 1, opening words and (b) of the Wbp.

[152] Dutch DPA z2010-00582, Definitive findings of the investigation by the Dutch DPA into the collection of WiFi data with Street View cars by Google, 27 December 2010, p. 19 and 25.
[153] Dutch DPA z2010-00582, Definitive findings of the investigation by the Dutch DPA into the collection of WiFi data with Street View cars by Google, 27 December 2010, p. 26-27
[154] Article 1, opening words and (b), of the Wbp defines – in full – the 'processing of personal data' as: '*any operation or set of operations which is performed upon personal data, such as, in any event, the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as the blocking, erasure or destruction of data*.' This paragraph is an implementation of Article 2, opening words and (b), of the Privacy Directive.

Elaboration of the legal framework

Article 1, opening words and (a) of the Wbp is an implementation of Article 2, opening words and (a) of the Privacy Directive:

> *'For the purposes of this Directive: "personal data" shall mean any information referring to an identified or identifiable natural person ("data subject"); an identifiable person is a person that can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.'*

Recital 26 of the Privacy Directive states in connection with this:

> *'Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the data controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; (...).'*

All data that can provide information on an identifiable natural person must be regarded as personal data.[155]

Data are personal data if by their very nature they concern[156] a person, such as factual or valuating data about attributes, opinions or forms of behaviour or – given the context[157] in which they are processed – they contribute to how the particular person is assessed or treated in society.[158] In the latter case, the use to which the data can be put contributes to answering the question of whether personal data are involved.[159] In addition, data that do not relate directly to a particular person but to a product or a process, for example, can furnish information about a particular person and are in that

---

[155] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 46.

[156] See Article 29 Working Party, Advisory opinion 4/2007 on the concept 'personal data' (June 2007), p. 10-11 and 27, URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf: *'Information "relates to" a person when it is "about" that person'*, in other words, the content. Idem, p. 11.

[157] Cf. idem, p. 11: Information 'relates to' a person *'when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual'*, in other words, the purpose.

[158] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 46. Cf. Article 29 Working Party, Advisory opinion 4/2007 on the concept 'personal data', p. 11: Information 'relates to' a person *'if its use, taking all the circumstances of the case into account, can be expected to have consequences for a person's rights or interests'*, in other words, the result.

[159] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 46. See also idem, p. 47: *'Contrary to what the Data Inspection Board states in its advice, it is not required that every possibility of using the data relating to persons be excluded. If this possibility does exist theoretically but it is inconceivable that it would actually occur, it can be assumed that the data are not considered personal data. If, on the other hand, it is possible to use the data to track down fraud, for example, then these data are personal data. Here, it is not relevant whether the intention to use the data for that purpose is also present. Data are already personal data when that data can be used for a purpose focused in such a way on the person'*, [underscore added by the Dutch DPA].

case personal data.[160] The legislative history of the Wbp cites the telephone number as an example.[161] The judgment from the Court of Justice of the European Union dated 24 November 2011 and the opinion from Advocate General Jääskinen dated 25 June 2013 cite the IP address.[162]

A person is identifiable if his identity can be determined, within reason, without disproportionate effort, directly or through further steps, by means of data that is so characteristic − in itself or in combination with other data − for that person.[163][164]
In order to determine whether a person is identifiable, it is necessary to examine all the means of which it may be assumed they can be used, within reason, by the data controller or any other person to identify that person.[165] This assumption must be based on a reasonably equipped data controller. [166] In concrete cases, however, it must be taken into account that the data controller has special expertise, technical facilities and the like at its disposal.[167]

---

[160] Idem, p. 46-47.
[161] Idem: *'In addition, (…) under certain circumstances telephone numbers (Data Inspection Board, 8 July 1993, 93.A.002) must be regarded as personal data.'* See also the Court of Justice of the European Union, 6 November 2003, case C-101/01 (*Lindqvist*), legal ground 27: '(…) *a reference to different people on an Internet page by name or otherwise, for example, with their telephone number or information about their work situation and their interests,* [can be, added by the Dutch DPA] *regarded as the full or partial automated processing of personal data in the sense of Article 3, paragraph 1, of Directive 95/46* (…)'.
[162] See the CJEU, 24 November 2011, case C-70/10 (Scarlet/Sabam), legal ground 26 and Opinion from Advocate General N. Jääskinen dated 25 June 2013, case C-131/12 (Google Spain SL and Google Inc./Agencia Española de Protección de Datos (AEP)), section 3 and footnote 48 on the status of IP addresses, which are personal data. In paragraph 3 the Advocate General writes: *'In the context of the Internet, three situations should be distinguished that relate to personal data. (...) The third, more invisible operation occurs when an Internet user performs a search using an Internet search engine, and some of his personal data, such as the IP address from which the search is made, are automatically transferred to the Internet search engine service provider.'*
[163] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 48. For example, *'cases (…) where data cannot be directly traced by name, yet the person can still be identified using the available means – for example, a number. This might include a situation in which a list of numbers and corresponding names is available, either through a public source (such as the telephone directory), or through a source that can only be consulted by a particular category of people (for example, the vehicle registration database by the police or a bank account number by bank employees). The data linked to those numbers are – although not by name – personal data because of the available option to use the numbers to ascertain the identity of the people involved.' Parliamentary documents II* 1998/99, 25 892, no. 13, p. 2.
[164] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 47-49. The legislative history of the Wbp contains the following remark on the term 'disproportionate effort': '*This would be the case, for example, if the identification of people by computer were to take many days.' Parliamentary Documents II* 1998/99, 25 892, no. 13, p. 2.
[165] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 48. Cf. also WP29 136, p. 16. Here, all the relevant factors must be taken into account, such as the costs of identification, the intended purpose of the processing, the way the processing is structured, the benefit expected by the party responsible for the processing, the interests at stake for the persons involved, the risk of organisational shortcomings (for example, breaches of the obligation to observe confidentiality) and technical malfunctions.
[166] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 48-49.
[167] Idem, p. 49. Data Inspection Board, 27 March 1995, 95.V.029.

In the legislative history of the Wbp, the following is added on the advancement of information technology: '*As advances are made in information technology, account must be taken of the fact that while in the past a disproportionate effort may have been required (and the data was not considered personal data therefore), this effort diminishes as new techniques become available. What can be regarded therefore as anonymous data at a particular point in time because they cannot reasonably be traced to a person – due to the state of the art at that point in time – can yet become personal data because of technical developments which increase the possibility that the data can be used to trace a particular person.*'[168]

Identification is also possible without finding out the name of the data subject. All that is required is that the data can be used to distinguish one particular person from others. The opinion of the Article 29 Working Party on the concept of 'personal data' includes the comment: '*(…) while identification through the name is the most common occurrence in practice, a name may itself not be necessary in all cases to identify an individual. This may happen when other "identifiers" are used to single someone out. Indeed, computerised files registering personal data usually assign a unique identifier to the persons registered, in order to avoid confusion between two persons in the file. Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. (...) In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name. The definition of personal data reflects this fact*', [underscore added by the Dutch DPA].[169]

When data are linked to a unique number, there is usually a case of an individual person. In that context, the Dutch DPA also refers to the consideration in the judgment of the Court of Justice of the European Union dated 6 November 2003 that '*(…) the act of referring, on an Internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes "the processing of personal data wholly or partly by automatic means" within the meaning of Article 3(1) of Directive 95/46.*'[170]

Data on the communication behaviour of the data subjects (for example, the content of e-mails and documents, films viewed, music listened to) are data of a sensitive nature.[171] That is true also of financial data, location details and information on surfing behaviour. In most cases the URL also has a content value, in the sense that it can provide information on the content of the communication.

The legal presumption in the cookie provision means that unless the placer/reader of tracking cookies demonstrates that he does not process personal data, he must satisfy the requirements of the Wbp.

[168] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 49.
[169] WP29 136. Advisory opinion 4/2007 on the concept of 'personal data' of 20 June 2007, p. 14-15.
[170] CJEU, 6 November 2003, case C-101/01 (*Lindqvist*), legal ground 27.
[171] *Parliamentary Documents II* 2000/01, 27 460, no. 2, p. 61. Idem, no. 1, p. 27.

Assessment

In section 3.3 of this report, the Dutch DPA ascertained that Google combines data on the use of its services in various devices and systems, specifically:
1. with regard to **authenticated users**, all data that are associated with an account (including name, e-mail address, cookies relating to the UserID, IP address and other registration data and usage (time and frequency) of Google services, including the contents of content uploaded, entered and received and sent by the user himself), can be used by any other Google service. This also relates to, for example, the location details of mobile devices, the unique device identifiers including IMEI number, browser and device settings, content of search queries and visits to third-party websites (via clicking on the +1 button or visiting websites with DoubleClick advertisements and/or Analytics code. Google states that for authenticated users it does not link the DoubleClick cookies to the data that can directly identify the user and that it does not collect any unique device identifiers with the DoubleClick cookies but this does not change the fact that Google does collect the device identifiers in the event of visits to and use of (other) Google services. In section 3.6, the Dutch DPA ascertained that Google also actually combines data on and from the use of various services. This includes combining data on visits to third-party websites with Google advertisements, apps used and the Google or YouTube profile in order to tailor advertisements via third-party websites.

2. with regard to **unauthenticated users**, data that are collected using the PREF, NID, DoubleClick and/or Analytics cookies and the IP address can be combined with data on the use of 'open' services from Google and third-party websites and used by any other Google service. In section 3.6, the Dutch DPA ascertained that Google actually combines data on the use of different services, for instance it combines data on the use of YouTube with other open services.

3. with regard to **passive users**, data collected using DoubleClick and/or the Analytics cookies together with the IP address can be combined with data on visits to websites on which these cookies are placed and read, including the URL referrers.

4.2.1 Legal presumption and cookies on Google's own websites (authenticated and unauthenticated users)

Search, Maps and YouTube are different information society services. If cookies are used to collect, combine or analyse data on the use of various information society services for commercial purposes, the legal presumption that tracking cookies process personal data, as contained in Article 11.7a of the Tw, applies.

The definition of 'information society service' goes back to, *inter alia*, directive 1995/34/EC on a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services (see also recital 17 of Directive 2000/31/EC on e-commerce). The definition covers all services normally provided for remuneration[172], at a distance, by electronic means, and at the individual

[172] Services for which the customers do not pay are also covered by the definition, as long as these represent a certain value in commerce. *Parliamentary Documents II* 2001/02, 28 197, no. 3, p. 12.

request of a recipient of a service.[173] Recital 18 of the directive on electronic commerce cites *various examples* of information society services, which encompass a great variety of economic activities that take place online: the offering of products and services via websites, the offering of search engines or storage services, the offering of video-on-demand and e-mail services.[174]

Google uses the PREF and NID cookies via its own websites (Search, Maps and YouTube) to collect data on the use of multiple information society services. According to Google, in the case of unauthenticated users both the PREF and NID cookies are used to tailor advertisements and for reporting purposes.[175] The PREF and NID cookies that Google places on its own websites are tracking cookies, therefore. This also applies for the DoubleClick cookies that are placed on YouTube, since the unique identifier in these cookies is also read out by all other websites that the users visit with DoubleClick advertisements. Pursuant to the legal presumption these are personal data.

With regard to the Analytic cookies that Google places and reads via its own websites (see section 3.3.1 of this report), these are personal data for Google (with regard to both the authenticated and the unauthenticated users). The Dutch DPA was and is aware of the fact that with Analytic cookies, Google uses a different identifier for each website, as also evidenced by previously published investigation into the use of Google Analytic cookies by TP Vision.[176] However, this does not change the fact that Google automatically collects the cookie identifier (with IP address, time, presumed location (to the level of city), browser properties and the URL referrer[177]) with the

[173] '"*Service": any information society service, i.e. any service normally provided for remuneration, by electronic means, at a distance and at the individual request of a recipient of a service*', Article 1(2) of the directive on a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services.

[174] '*Information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data. Information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service. (...) by contrast, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services. (...)*', recital 18 from the directive on electronic commerce.

[175] Google's written view, paragraph 57.

[176] Dutch DPA, z2012-00605, Public version of the Report of definitive findings of investigation into personal data processing with or by a Philips smart tv by TP Vision Netherlands B.V., July 2013, p. 57-58, URL: http://www.cbpweb.nl/downloads_pb/pb_20130822-persoonsgegevens-smart-tv.pdf

[177] '*The HTTP request for any web page contains details about the browser and the computer making the request, such as the hostname, the browser type, referrer, and language. In addition, the DOM of most browsers provides access to more detailed browser and system information, such as Java and Flash support and screen resolution. Analytics uses this information in constructing reports like the Map Overlay, Browser, and Referring Sites reports. Analytics also sets and reads first-party cookies on your visitors' browsers in order to obtain visitor session and any ad campaign information from the page request. The Google Analytics Tracking Code also reads the double-click cookie to inform Google Analytics for Display Advertisers.*' Source: Google ' How Does Google Analytics 11 november 2013

placement and reading of Google Analytic cookies on its own various websites. It is important here that Google does not state or declare anywhere that it deletes the last octet of the IP address also for itself. To the extent that, in accordance with its privacy policy, Google combines the Analytics data with data on DoubleClick cookies for retargeting purposes and with data on social media use (Social Analytics), these are also tracking cookies to which the legal presumption from Article 11.7a of the Tw applies.

4.2.2 Legal presumption and cookies via third-party websites (all three types of users)

The DoubleClick cookies that Google places and reads via third-party websites are tracking cookies aimed at monitoring individual surfing behaviour across multiple websites and displaying personalised ads based on that. Pursuant to the legal presumption from Article 11.7a of the Tw, these are personal data.

In its written view Google points out that the legal presumption concerning tracking cookies contained in Article 11.7a of the Tw is a rebuttable presumption. It does not alter the criteria for determining whether particular data are personal data. Since Google does not have any access to real means for identifying unauthenticated and passive users, it does not believe these are personal data. Google says that combining an IP address with PREF cookies and search terms does not make these data personal data. Although Google does have many employees and computer equipment, this does not justify the general conclusion that Google can identify unauthenticated users. Though Google can target its services at an unauthenticated user by means of a cookie ID, it says that it cannot identify the user of the device.[178]

Article 11.7a of the Tw contains a legal presumption concerning tracking cookies. This legal presumption is not rebutted with the (otherwise unsubstantiated) statement that Google does not have access to real means for directly or indirectly discovering the user's identity. The criterion is not that Google does not 'know' who the user is, but whether Google or any other party can reasonably trace the user's identity.

The term personal data not only encompasses identification by the data controller, but also identifiability, whether or not through intermediary steps, by or via a third party. It is important here that third parties such as advertisers have the motive of selling a service or product and therefore of obtaining the contact details of the particular Internet user (in the event of actual purchase of the product or service). Advertisers in fact use Google's advertising network comprising more than 2 million websites and apps to obtain detailed interest profiles and employ personalised ads to tempt specific users to buy the advertised products and services.[179]

Collect Data?', URL: https://developers.google.com/analytics/resources/concepts/gaConceptsTrackingOverview?hl=en#howAnalyticsGetsData (URL last visited on 29 October 2013).

[178] Google's written view, paragraphs 19-22 and 42.

[179] The publication on 4 October 2013 in the English newspaper The Guardian of (the analysis of) a Powerpoint presentation from the NSA showed, incidentally, that the US National Security Agency (NSA) places DoubleClick cookies in the browsers of TOR users with the specific objective of being able to identify them. URL of analysis by Bruce Schneier: http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-

By stating that such data relating to unauthenticated (and passive) users are not personal data, without indicating with substantiation why the legal presumption does not apply, Google takes the position that European privacy rules do not apply to many of its services. As such Google overlooks the fact that the legal presumption in the Tw relates precisely to the privacy impact of charting out surfing and search behaviour by means of cookies and other tracking methods for commercial purposes.[180]

Since Google has not adequately substantiated that traceability by it or a third party is not reasonably possible, the Dutch DPA does not consider the legal presumption in relation to the tracking cookies used by Google to be rebutted.

The Analytic cookies that Google places and reads from the (browsers on the) end-user terminal equipment of unauthenticated and passive users (with the aid of JavaScript) via third-party websites are also personal data. In its written view Google disputes that Analytic cookies are personal data because these are first-party cookies with a unique identifier per website and the cookies are set up under the Google Analytics client's domain.[181] Google also writes in its written view: '*Google does not monitor the surfing behaviour of individual users who visit websites that use different Google Analytics accounts.*'[182]

It is a fact, however, that through the use of Analytic cookies via third-party websites Google itself automatically collects the cookie identifier (with IP address, time, presumed location (to the level of city), browser properties and the URL referrer). In relation to this Google has declared and it has emerged from investigation that it is possible for website owners to disable the functionality 'share data' with Google. Furthermore, website owners can ask Google to delete the last octet of the website visitor's IP address immediately after collection. Any masking of the last octet of the IP address at the request of website owners does indeed result in diminished traceability (a group of usually 254 different users maximum), but, because of the presence of additional data such as time and URL referrers, no disproportionate effort

---

online-anonymity. Powerpoint presentation: http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document, p. 8-9.

[180] '*When personal data are processed using cookies, in particular by the use of third-party cookies for behavioural advertising, the user himself must make an explicit choice'*, and: '*Even if it cannot be proven that personal data, in the strict sense of the word, are collected or processed, the operations referred to are designated as the collection or processing of personal data. As such the more stringent regime of the Wbp applies for this category of operations, of which the placement and reading of so-called tracking cookies is the best known. That is to say, the user must grant unambiguous consent.'* Notes to the amendment, further amended, from members Van Bemmel and Van Dam to the Amendment of the Telecommunications Act, *Parliamentary Documents II* 2011/12, 32 549, no. 39. Cf. also the notes from the Minister of Economic Affairs to the Lower House on the legal presumption: *'The legal presumption that the Lower House has added to the cookie provision reverses the burden of proof, making it easier for the Dutch Data Protection Authority to effectively supervise compliance with the Wbp in relation to tracking cookies.' Parliamentary Documents II* 2011/12, 32 549, no. 47, letter dated 8 March 2012.

[181] Google's written view, paragraph 47.

[182] Idem.

is necessary during Google's collection of the data to trace the surfing behaviour to an individual data subject.[183]

Google points out to clients that it uses the Analytics data in accordance with its privacy policy and can therefore use the data for its own purposes, such as product development and analytics. Furthermore, since Google's default setting is that website owners consent to Google's combining of Analytic cookies with DoubleClick cookies[184] and Google also enables website owners (and by extension itself) to have the Analytics data enriched with data from authenticated users on their interaction with social media, these are, in a legal sense, tracking cookies in these cases as well, as explained in the Article 29 Working Party's opinion on consent for cookies.[185] The legal presumption from Article 11.7a of the Tw that these are personal data applies to these tracking cookies.

4.2.3 Data 'relating to' a person

The Google account (with accompanying PREF cookies and cookies relating to the UserID), the IP address, the DoubleClick cookies, data on clicked +1 buttons, the IMEI numbers and MAC addresses of smartphones (unique client and/or device identifier(s)), in and of themselves or in combination with each other or in connection with (technical and content) data on the visit to and use of Google services and third-party websites, including information on the settings of the (browser on the) device and websites visited earlier via the URL referrers, are by their very nature data on the behaviour of a natural person (information on his Internet use).[186]

Google can, and in fact does, in practice, use these data to treat the data subject in a particular way or influence the behaviour of that person, in a way that has consequences for the data subject's rights/interests. This could for instance include personalising search results for both authenticated and unauthenticated users on grounds of earlier search behaviour or information on the use of other services, the setting up of profiles for all three types of users for advertising purposes and the displaying of personalised ads on the basis of these Internet behaviour profiles, as well

[183] See also the letter to Google from the Article 29 Working Party dated 26 May 2010, URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_05_26_letter_wp_google.pdf. Cf. also the conclusions from the investigation by the joint German privacy regulators into the conditions under which Google Analytics can be used lawfully. Statement from Datenschutz Hamburg, 'Beanstandungsfreier Betrieb von Google Analytics ab sofort möglich', 15 September 2011, URL: http://www.datenschutz-hamburg.de/news/detail/article/beanstandungsfreier-betrieb-von-google-analytics-ab-sofort-moeglich.html

[184] *The Google Analytics Tracking Code also reads the double-click cookie to inform Google Analytics for Display Advertisers'.* Source: Google ' How Does Google Analytics Collect Data?', URL: https://developers.google.com/analytics/resources/concepts/gaConceptsTrackingOverview?hl=en#howAnalyticsGetsData.

[185] Article 29 Working Party, Opinion 04/2012 on Cookie Consent Exemption (June 2012), URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

[186] Information can be derived from these data about the communication behaviour of the data subject and sometimes also about the content of the communication.

as the analysis of the substance of content and communication-oriented services such as Gmail and Drive in order to display personalised ads.

Google therefore uses the data in a way that affects the data subject in society.

Furthermore, the Internet use of a data subject can provide clues, for example, about his interests, social background, income or family structure. Such information can be used for (direct) marketing and profiling purposes.[187]
Whether it is Google's intention to use the data about and from the data traffic for either those purposes or other purposes is not of overriding importance. The data can already be regarded as personal data if they can be used for this type of purpose aimed at the individual, and this possibility is present. In the legislative history of the Wbp, the following is noted in this context: *'If, on the other hand, it is possible to use the data to track down fraud, for example, then these data are personal data. Here, it is not relevant whether the intention to use the data for that purpose is also present. Data are already personal data when that data can be used for a purpose focused in such a way on the person.'*[188] The use for a purpose focused on the person is possible.

4.2.4 Identifiability of the person

The data on and from the data traffic are, in and of themselves, in combination with each other or in connection with information originating from another source, directly or indirectly traceable by Google to an identifiable natural person (users of its Internet services).

Authenticated users

When registering for a Google account, users are asked to give their name, date of birth and mobile telephone number. Only the name and e-mail address are required. According to its privacy policy, Google attempts to discover a user's 'real' name by comparing the name given with names used in other services. When creating an account, users can either create a (new) Gmail e-mail address or use an existing e-mail address. Here Google also automatically obtains the IP address with which the user is creating an account and places a PREF cookie. So for authenticated users, Google has in any event an IP address, an e-mail address, a PREF cookie and name details (correct or otherwise). In many cases Google also has a mobile telephone number. These data are personal data as explained (in relation to the telephone number and e-mail address of natural persons, explained specifically in the legislative history of the Wbp and the Tw) in various opinions from the Article 29 Working Party and (with regard to the IP address) confirmed for Google by the Advocate General of the CJEU[189] and more generally by the CJEU in the Scarlet/Sabam case.[190]

[187] Definitive findings of the investigation by the Dutch DPA into the collection of WiFi data with Street View cars by Google of 7 December 2010, p. 35 (z2010-00582). URL: http://www.cbpweb.nl/Pages/pv_20110913_google.aspx.
[188] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 47.
[189] See p. 43 of this report.
[190] CJEU, 24 November 2011, case C-70/10 (Scarlet/Sabam), legal ground 26.

As a result of the use of Google services like Google+, Search, Gmail and Drive, Google also obtains additional data such as the content of search queries (including so-called vanity searches in which people search for their own name), the content of the Google+ profile, content of e-mails and contacts, and the content of documents that are created or read via Drive. Google also collects data on the settings of the (browser on the) device and/or data about the mobile device (the model, browser type or sensors such as the accelerometer, as well as the IMEI number and the apps installed on the device) which the users use to surf, the most recent URL visited (the referrer), and the location details via the use of a service like Maps. If an authenticated user enables location details on his Android smartphone, he automatically discloses to Google where he usually sleeps and therefore also where he most likely lives.

Authenticated users can also use services like Wallet, Google Play to install apps and Voice. Via these services Google can collect additional personal data, such as credit card and payment data, and it obtains data about the installation and use of apps and telephone numbers.

With regard to authenticated users who use Google's services on a smartphone or tablet, hashing the unique advertisement identifier and then linking it to a new identifier does not prevent Google from approaching the individual user with personalised ads. Every time such a user sees a Google advertisement, Google can link new data to this new identifier. That is why use of this pseudonymisation method does not lead to the conclusion that the data are no longer personal data.[191]

Finally, Google can collect data on authenticated users' visits to third-party websites using DoubleClick and Analytic cookies and if authenticated users click on a Google +1 button. Google uses these cookies to collect data on visits to multiple websites, including the time, frequency and URL referrer.

For authenticated users, therefore, in its databases/files Google has a combination of directly and indirectly identifying data arising from the use of its services, also via third-party websites.

The Dutch DPA further takes into account that as evidenced by its privacy policy, Google may combine all the data mentioned above for the purpose of displaying personalised ads and is capable of comparing the name given by the user to data in other services. Data processing for these purposes is only worthwhile if it enables

[191] For the Dutch DPA's earlier assessments of hashing methods and the use of pseudonyms, see z2011-00462, Investigation into the analysis by Tele2 Nederland B.V of data on and from mobile data traffic (29 May 2013), URL: http://www.cbpweb.nl/downloads_rapporten/rap_2013-analyse-gegevens-mobiel-dataverkeer-tele2.pdf, Z2011-00987, Investigation into the processing of personal data for the 'whatsapp' mobile application by WhatsApp Inc. (January 2013), URL: http://www.cbpweb.nl/downloads_rapporten/rap_2013-whatsapp-cbp-definitieve-bevindingen-nl.pdf, and the Dutch DPA's official investigation into the processing of geolocation data by TomTom N.V. (20 December 2011), URL: http://www.cbpweb.nl/downloads_pb/pb_20120112_tomtom-geolocatie-persoonsgegevens-definitieve-bevindingen.pdf).

recognition of specific persons and the different treatment of these persons by showing them different advertisements. Since Google in any event has an e-mail address and IP address (and in many cases, a mobile telephone number), Google can approach the data subjects directly and the data must therefore be regarded as personal data as referred to in Article 1(a) of the Wbp.

The personal data (information) relating to the content of received and sent e-mails, personal profiles and documents of data subjects are data of a sensitive nature. This is also true of location details, surfing and search behaviour.

Unauthenticated users
When a user uses 'open' Google services like Search, Maps or YouTube, Google automatically obtains the user's IP address. When these services are used Google also places (and reads) PREF, NID, and in many cases Analytics cookies as well, and (for YouTube) DoubleClick cookies. For unauthenticated users, therefore, Google has in any event an IP address, a PREF and NID cookie, and user data on these services, such as search queries, locations searched for and films viewed. Google also collects data on the settings of the (browser on the) device and/or data about the mobile device (the model, browser type or sensors such as the accelerometer) which the users use to surf and the most recent URL visited (the referrer). If unauthenticated users visit third-party websites with Google advertisements, Google collects data on their surfing behaviour using Analytics and DoubleClick cookies.

Identification is also possible without finding out the name of the data subject. All that is required is that the data can be used to distinguish one particular person from others, as explained in the Article 29 Working Party's opinion on the concept of 'personal data' (see p. 43 of this report). When data are linked to a unique number, this usually involves an individualised person.

For unauthenticated users, therefore, in its databases/files, Google has a combination of directly and indirectly identifying data arising from the use of its services. The efforts that Google must expend to (be able to) trace these data to an individual natural person are not disproportionate. Google employs many technicians skilled in this area and has the necessary technical facilities (including applications to query the databases and the technical capability to export data from these databases) to link the data to each other or, if necessary, to go through intermediate steps to trace the data to the particular unauthenticated user.

In its written view, Google writes that in order to qualify as personal data, it is not sufficient that a person can be distinguished from another person, but that it must be reasonably possible to find out that person's identity. Google writes that it does not know who a particular user is and does not have access to real means to trace IP addresses and other unique codes or numbers (from a device, application or cookie) to an identified user.[192] According to Google, the judgment of the Court of Justice of the EU in relation to IP addresses (in the Scarlet/Sabam case), cited by the Dutch DPA, relates to traceability by Internet access providers, who themselves assign IP addresses

[192] Idem, paragraph 20.

to their clients and have a contractual and invoicing relationship with these clients. According to Google this case does not mean that IP addresses must also be regarded as personal data in the context in which Google processes these data.[193] Furthermore, Google writes, an IP address can be shared by multiple devices in a household and individual devices are often used by several people: '*When mobile devices are connected to the Internet via the mobile network, even thousands of devices can be hiding behind the same IP address.*'[194]

The Dutch DPA does not refer only to the Scarlet/Sabam case as substantiation for the view that IP addresses are personal data, but also to earlier investigations by the Dutch DPA and publications from the Article 29 Working Party. It was ascertained in the Scarlet/Sabam judgment that the IP addresses were personal data for the ISP. Because the definition of personal data is based on identifiability by the data controller or any other party, IP addresses are therefore personal data. Furthermore, the Dutch DPA points to the Advocate General's advice in the Google/AEPD case in which he states, without any nuance, that IP addresses are personal data, precisely in the specific context of Google which, as search machine, collects IP addresses and accompanying data on search behaviour.[195] Added to this is the fact that the definition of personal data that can be used to directly or indirectly identify someone in Article 2(a) of the Privacy Directive (95/46/EC) makes specific reference to an identification number. IP addresses are such identification numbers (as are permanent cookies with unique identifiers). Sections 4.2.1 and 4.2.2 of this report discuss in more detail the identifiability of personal data that are collected using tracking cookies.

The fact that an IP address can be used by multiple devices and devices can be used by several people does not change the fact that personal data are indeed involved here. A fixed telephone can also be used by several people in the household, as can a car, for instance. Also according to the parliamentary history of the Wbp[196], this does not preclude the conclusion that personal data relating to an identifiable person are concerned if the data on the use are attributed to the owner of the telephone or car.

Google's defence that no personal data are involved in the use of unique codes and numbers (whether or not in combination with IP addresses) furthermore logically contradicts the nature of the personalised services and advertisements. It is a fact that Google offers personalised services to active users and personalised ads to all three

[193] Google's written view, paragraphs 14-17 and 20.
[194] Google's written view, paragraph 18.
[195] Opinion from Advocate General N. Jääskinen dated 25 June 2013, case C-131/12 (Google Spain SL and Google Inc./Agencia Española de Protección de Datos (AEP)), URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=NL&mode=lst&dir=&occ=first&part=1&cid=417901, paragraph 3: '*In the context of the Internet, three situations should be distinguished that relate to personal data. (...) The third, more invisible operation occurs when an Internet user performs a search using an Internet search engine, and some of his personal data, such as the IP address from which the search is made, are automatically transferred to the Internet search engine service provider.*'
[196] *Parliamentary Documents II* 1997/98, 25 892, no. 9, p. 2. '*After all, it is plausible that such use of the data has or could have consequences for the person with whom the telephone number is linked. A situation that is similar to this to a certain extent can occur with the use of car number plates.*'

types of users. This means that individuals can evidently be effectively approached and can be treated differently even if their individual names are not known. It is significant here that in the Lindqvist judgment it was accepted that in order for a person to be identifiable, his name need not be known.[197] If, via its advertisements, Google were to constantly recommend products or services based on a 'different' person's Internet behaviour, someone with very different interests, the personalised advertising would be of very limited use for Google. Furthermore, Internet behaviour (as recorded via, among other things, cookies with unique identifiers) can provide clues on the family situation (presence of children, for instance), which can be used to effectively and specifically approach the decision maker in the household (the likely owner of the particular device and/or subscriber to whom the IP address has been assigned). Via the personalised ads, the consequences of use of a single IP address and/or a single device by several people are effectively attributed to the owner of the IP address/owner of the device.[198] The Dutch DPA also refers to the recent opinion from the Berlin group of international privacy regulators on Web Tracking and Privacy.[199] This clearly describes that the purpose of displaying personalised ads is to sell products or services to people, not to devices:

'*While ads may well be addressed to a machine at the technical level, it is not the machine which in the end buys the proverbial beautiful pair of red shoes - it is an individual. Thus, the claim that the processing of behavioural data for marketing is directed "only" at machines in the first place may well be seen as an attempt to blur our vision as societies on the gravity of the problem, when in reality the individual and not the machine is the only instance that can make all such tracking operations a "success" for its proponents (i.e., when the red shoes are finally being bought).*'[200]

The comment that IP addresses on mobile networks can be shared by thousands of different mobile devices overlooks the fact that Google precisely uses all sorts of unique device identifiers, data about the particular device and (where possible) cookies with unique numbers in combination with the IP addresses in order to recognise the individual devices. In relation to device IDs, for example, Google writes: '*A unique device ID is a series of characters that is included in a device by the manufacturer and can be used to uniquely identify that device. Different device IDs vary in the extent to which they are permanent or can be restored by users and how they can be opened. A particular device can have a few different unique device IDs. Unique device IDs can be used for various*

[197] CJEU, 6 November 2003, case C-101/01 (*Lindqvist*), legal ground 27.
[198] Cf. also the Dutch DPA's assessment of a similar defence from TP Vision Netherlands B.V., the producer of Philips smart televisions, that televisions can be used by several people in a household and that for that reason data on television behaviour are allegedly not personal data. Dutch DPA, z2012-00605, Public version of the Report of definitive findings of investigation into personal data processing with or by a Philips smart tv by TP Vision Netherlands B.V., July 2013, URL: http://www.cbpweb.nl/downloads_pb/pb_20130822-persoonsgegevens-smart-tv.pdf
[199] International Working Group on Data Protection in Telecommunications, Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential (15 and 16 April 2013, Prague, Czech Republic, URL: http://www.datenschutz-berlin.de/attachments/979/675_46_32.pdf?1379937149.
[200] Working Paper on Web Tracking and Privacy, p. 3, paragraph 11.

purposes, including security and fraud detection, to synchronise services such as a user's inbox, to remember a user's preferences and to offer relevant advertisements [underscore added by the Dutch DPA].'[201] This actually means that Google collects the MAC address of the smartphone and the IMEI number, as well as unique identifiers added by the manufacturer of the operating system, such as the AdID on iOS.

Where cookies are not possible (for instance in apps on mobile devices), Google uses 'anonymous IDs'. Google writes concerning this: *'In order to display advertisements in services in which cookie technology may not be available (for example, in mobile apps), we can use anonymous IDs. These carry out functions that are similar to those of cookies.'* An 'anonymous ID' is defined by Google as follows: *'An anonymous ID is a random series of characters that is used for the same purposes as a cookie on platforms where cookie technology is not available, which includes certain mobile devices.'*[202]

Because the concept of identifying is not limited to knowing an individual's name and because the purpose of Google's processing can only be achieved if it can trace the individual users, Google is considered to have the real means to be able to identify them. Whether Google knows the names of the data subjects is not relevant here.

Additionally, Google can, in some cases, also trace the user's name if this person performs a vanity search or, for instance, marks his home location when using a service (or app) like Maps. In its written view Google writes in relation to this that it can only know that a search is a 'vanity search' if it knows the user's identity.[203] With regard to these 'vanity searches', the Dutch DPA points out that the majority of Internet users do search for their own names in search engines at some point[204] and that this is not just vanity, but a highly recommended method for checking what other people see if they search for your name, for example when you are applying for jobs.[205] It is also a fact that it was ascertained in 2006 already, after the release of a large number of search queries in combination with a unique number per user by US Internet provider AOL[206] that certain individuals could in fact be identified by the

[201] Google Policy and Principles, hyperlink 'Key terms', URL: http://www.google.nl/intl/nl/policies/privacy/key-terms/#toc-terms-unique-device-id (forensically recorded by the Dutch DPA on 11 July 2013).
[202] Google Policy and Principles, hyperlink 'Key terms', URL: http://www.google.nl/intl/nl/policies/privacy/key-terms/#toc-terms-identifier (forensically recorded by the Dutch DPA on 15 July 2013).
[203] Google's written view, paragraph 21.
[204] A recent study by the US-based Pew Research Center indicates that 56% of (US) Internet users have searched for their own names. PewInternet, '56% of Internet Users Have Searched for Themselves Online', 27 September 2013, URL: http://pewinternet.org/Media-Mentions/2013/56-percent-of-Internet-Users-Have-Searched-for-Themselves-Online.aspx (URL last visited on 29 October 2013).
[205] See for example Intermediair, 'Solliciteren? Google jezelf naar binnen!', 4 April 2013, URL: http://www.intermediair.nl/vakgebieden/it-internet/solliciteren-google-jezelf-naar-binnen (URL last visited on 29 October 2013).
[206] See for example, The New York Times, 'A Face Is Exposed for AOL Searcher No. 4417749', URL: http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482 (URL last visited on 29 October 2013).

combination of vanity searches with other search queries. This is much easier (for Google and for third parties) in combination with the IP addresses. It is also a fact that in earlier court cases Google itself in fact acknowledged the importance of privacy in relation to search queries precisely because sensitive personal data appear in these.[207] In the court case brought by the US Department of Justice against Google in 2006 concerning Google's refusal to provide a great number of search queries, Google declared: *'There are ways in which a search query alone may reveal personally identifying information.'*[208]

The Dutch DPA also takes into account that as evidenced by its privacy policy, Google can combine all the above-mentioned data from unauthenticated users for the purposes of personalising services like Search and YouTube and for displaying personalised ads elsewhere on the Internet. In section 3.6, the Dutch DPA ascertained that Google actually combines the data mentioned for these purposes.

Data processing for this purpose is only worthwhile if it enables recognition of specific persons and the different treatment of these persons by showing them different search results and advertisements. Since Google in any event has an IP address and unique NID and PREF cookies (and for YouTube, also has DoubleClick cookies) and has the unique identifier that is linked to the hash of the advertisement identifier on the mobile devices, Google can approach the data subjects directly and the data must therefore be regarded as personal data as referred to in Article 1(a) of the Wbp.

The personal data (information) on the search behaviour and website visits of data subjects are data of a sensitive nature. This is true also of (raw) location details (calculated for the IP address).

Passive users

Google collects data on Internet users via third-party websites, either for the purpose of website analytics or to be able to display personalised ads via DoubleClick. This at least includes the IP addresses of these website visitors and one or more cookies, in combination with the URLs of the websites visited and previously visited URLs with the same cookies. Google also collects data on the settings of the (browser on the) device which the users use to surf. With regard to these passive users, Google has the combination of IP address, cookies and use data (the websites that allow the

[207] At the beginning of 2006 Google refused to hand over a large number of search queries to the US Department of Justice, partly because of the privacy interest of users. See: The Guardian, Google refuses White House search request, 20 January 2006, URL: http://www.theguardian.com/technology/2006/jan/20/searchengines.usnews (URL last visited on 9 October 2013). In July 2013, Google offered a settlement of 8.5 million dollars in two consolidated class action cases from users who complained that their search queries, including specific vanity searches, had been passed on to third parties via the URL referrers without their consent. See for example MediaPost, 'Google To Settle 'Data Leakage' Case For $8.5 Million', 22 July 2013, URL: http://www.mediapost.com/publications/article/205047/#axzz2hDZPbK54 (URL last visited on 9 October 2013).

[208] Declaration of Matt Cutts in 'Gonzales v. Google', 234 F.R.D. 674 (N.D. Cal. 2006) p. 9, URL: http://docs.justia.com/cases/federal/district-courts/california/candce/5:2006mc80006/175448/14/0.pdf.

DoubleClick and Analytics cookies to be placed and read by Google, and whether the user has clicked on the advertisements displayed). For users of mobile devices, Google has the combination of IP address, advertisement use data and the unique identifier that is linked to the hash of the advertisement identifier.

In view of the foregoing, including the written view from Google discussed under the heading 'unauthenticated users' and the Dutch DPA's response to that, the data cited in this section, originating from passive users of Google services, are, in and of themselves (specifically: the IP address, the cookie(s) and the mobile device identifier(s)), in combination with each other or in connection with data on visits to third-party websites, personal data as referred to in Article 1(a) of the Wbp. The personal data (information) on the Internet behaviour of data subjects are data of a sensitive nature.

4.3 Processing personal data

Elaboration of the legal framework

The concept of 'processing personal data' as referred to in Article 1, opening words and (b) of the Wbp encompasses the entire process that personal data undergo from the moment they are collected until the moment they are destroyed.[209] Generating personal data is also processing.[210] The collection of data need not be accompanied by the recording of these data.[211] Fully automated forms of data processing are also processing, as long as (any) influence can be exerted thereon.[212]

Assessment

Google has declared that it processes (personal) data as referred to in Article 2(b) of the Privacy Directive. *'In the course of providing its services, Google undertakes a full range of processing operations and/or sets of operations consistent with the definition of "processing" set out in Directive 95/46/ EC. Such operations include, consistent with the Directive's definition: the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking and erasure or destruction of data.'*[213]

In section 3.4, the Dutch DPA ascertained that Google obtains (collects) and combines the personal data in any event for the four purposes investigated in this report :

[209] See *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 52.
[210] Idem, p. 51.
[211] Collection already takes place even if the data are obtained and subsequently immediately destroyed. *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 68.
[212] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 51-52: *'As soon as there is any actual power over personal data, the legislative proposal applies. Human intervention is not always required for this to be the case. Fully automated forms of processing can also fall under the legal regulation. What remains crucial is that the processing must be accompanied by the possibility of exercising (some) influence thereon. It is not relevant whether the influence is actually exercised. (...) If, however, an Internet service provider, for example, has the ability to prevent the dissemination of unlawful messages, there is a case of potential influence and as such a case of data processing, and because of that the law fully applies.'*
[213] Letter from Google to the CNIL dated 21 June 2012, answer to (the repeated) question 5.

1. personalisation of requested services;
2. product development;
3. display of personalised ads; and
4. website analytics.

In view of the foregoing, Google processes personal data as referred to in Article 1(b) of the Wbp.

4.4 Specific and legitimate purposes

Elaboration of the legal framework

Article 7 of the Wbp stipulates: *Personal data are collected for specific, explicitly described and legitimate purposes.*

'Specific and explicitly described' means that a party may not collect any data without an exact specification of its purpose in doing so.[214]

'Specific' entails that the purpose specification must be clear (not so vague or broad that during the collection process it cannot provide any framework against which it can be tested whether the data are necessary for that purpose or not).[215] The purpose may also not be formulated in the course of the collection process.[216] '*More generally it can be noted that the collection of data on arbitrary citizens for a purpose that may be relevant in the future is, in principle, not permitted. Gathering personal data exclusively "because these may be handy in the future" or "because you never know" is not permitted therefore.*'[217]

In its opinion on the purpose limitation, the Article 29 Working Party writes: *'For these reasons, a purpose that is vague or general, such as for instance "improving users' experience", "marketing purposes", "IT-security purposes" or "future research" will – without more detail – usually not meet the criteria of being "specific".'*[218]

The legislative history shows that there can only be 'legitimate purposes' if these can be achieved with due observance of Article 8 of the Wbp (legal ground). '*The realisation of these purposes must, in all stages of the data processing, be able to rely on one or more of the grounds for data processing cited in Article 8. If, for example, a purpose can only be achieved if personal data are stored in breach of Article 8 or are provided to a third party, the requirement of a "legitimate purpose" is not satisfied and the particular data may, on grounds of Article 7, also not be collected.'*[219]

Therefore, the data processing must be able, in all stages of the data processing, to rely on one or more of the legal grounds cited in Article 8 of the Wbp.

---

[214] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 79.
[215] Idem.
[216] Idem.
[217] *Parliamentary Documents II* 1997/98, 25 892, no. 6, p. 34.
[218] Article 29 Working Party, Opinion 03/2013 on purpose limitation (April 2013), p. 16, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[219] Idem.

Assessment

In GPP2012, Google writes: *'We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you personalised content – like giving you more relevant search results and ads.'* Upon the introduction of GPP2012 Google stated that the purpose was to recognise an (authenticated) user as the same user in all services, in order to ensure an easier, more intuitive Google experience.[220] Google wrote to the CNIL: '*Given the way in which our services (and the Internet in general) work, our processing for each of these purposes generally involves varying combinations of processing operations. We believe that our approach to describing how we use information is consistent with other major Internet companies.*'[221]

This report distinguishes and investigates four specific purposes for which Google collects and combines data, specifically: personalisation of requested services, product development, display of personalisedads, and website analytics.

In its written view, Google cites 'to provide the Google service' as the purpose for which data processing takes place. Google contests that data are processed for different purposes: '*This categorisation* [by the Dutch DPA, added by the Dutch DPA] *ignores Google's sole, primary objective in using personal data: to provide its online service to its users. Google collects data for that purpose (both when authenticated users initially create their Google Account and when users use the Google service) and subjects these to further processing for that purpose.*'[222]

The purposes investigated by the Dutch DPA not only involve the combining of personal data from authenticated users, however, which Google acknowledges to be personal data, but also the combining of personal data from unauthenticated and passive users. In answer to questions from the CNIL, in its written view submitted to the Dutch DPA and in GPP2012, Google repeatedly mentions services (the term 'services' appears 42 times in GPP2012). In GPP2012 Google also cites different purposes for the data processing. The Dutch DPA has investigated four of these actual purposes in this report.
Because the description of the purpose/the purposes for which Google collects data is not consistent and unequivocal, it is up to the Dutch DPA to investigate and determine the actual purposes of the data processing. The Dutch DPA also refers here to the opinion of the Article 29 Working Party on purpose limitation: '(...) *where the purposes are specified inconsistently or the specified purposes do not correspond to reality (…), all factual elements, as well as the common understanding and reasonable expectations of the data subjects based on such facts, shall be taken into account to determine the actual purposes.*'[223]

---

[220] *In short, we'll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience.'* Google Official Blog, 24 January 2012, URL: http://googleblog.blogspot.nl/2012/01/updating-our-privacy-policies-and-terms.html.
[221] Letter from Google dated 21 June 2012, in answer to question 5 from the CNIL.
[222] Google's written view, paragraphs 24-26.
[223] Article 29 Working Party, Opinion 3/2013 on purpose limitation, p. 19, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

In reality, for users there is no such thing as one Google service, but a range of services, whereby users deliberately choose to make use of one service but perhaps not of the other, and choose either to sign in or not to sign in, as Google itself also admits in its written view.[224]
To the extent that Google takes the position that 'to provide the Google service' is the overarching primary purpose of the processing, the Dutch DPA regards the four examined purposes in relation to authenticated and unauthenticated users as independent sub-purposes of this primary purpose. Where passive users are concerned, the Dutch DPA regards the three purposes that apply to these users as (independent) purposes existing alongside each other. Passive users have no contractual relationship with Google and for that reason, there can be no case of sub-purposes of the data processing for these users (for more on this, see section 4.6.3 of this report).

Google describes in GPP2012 that it may combine data from various services. '*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*.' It is also evident from the information about the Analytics service that Google can use data that it obtains via this service in accordance with its privacy policy. With reference to the opinion from the Article 29 Working Party on purpose limitation, the Dutch DPA concludes that such undetailed purposes are not specific and do not adequately detail the manner in which the personal data are processed. [225]

The purpose limitation principle excludes that personal data may be used for unexpected and incompatible new purposes. In connection with the transparency requirements, correct application of the purpose limitation principle results in 'surprise minimisation' for users.[226] That means that people who decide to deliberately use Google services (regardless of whether they do so as authenticated or unauthenticated users) must be able to understand in advance for what purposes Google collects the data and consequently be given control over whether they want to allow their data to be collected for those specific purposes. The purpose cannot be so vague or broad that during the collection process it cannot provide any framework against which it can be tested whether the data are necessary for that purpose or

[224] Google's written view, paragraph 74: '*A user can himself decide (...) whether or not to use a specific Google product like Gmail or Drive (...).*'
[225] See also Article 29 Working Party, Opinion 3/2013 on purpose limitation, p. 16 and 52: '(…) *a purpose that is vague or general, such as for instance "improving users experience", "marketing purposes", "IT-security purposes" or "future research" will - without more detail - usually not meet the criteria of being "specific".*' And: '*(…) In this case* [which involves a large company active throughout Europe that uses complex analytics to make tailored offers and advertisements, added by the Dutch DPA], *the purposes must be specified in a much more detailed and comprehensive way, including, among other things, "the way in which" personal data are processed.*'
[226] Term taken from the Warsaw Declaration on the appification of society, as adopted during the annual international meeting of data protection commissioners in Warsaw on 24 September 2013, URL:
http://www.priv.gc.ca/information/conf2013/declaration_e.asp
11 november 2013

not.[227] Collecting personal data for a purpose to be determined in the future, 'because you never know', is, in principle, not permitted therefore.

With regard to the purposes cited by Google, neither users nor regulators can automatically conclude from the purpose specification 'to provide the Google service', in connection with the statements in GPP2012, that Google combines and processes all sorts of data originating from and about the use of various Google services for purposes which, from the user perspective, are as diverse as the display of personalised ads, product development or the personalisation of requested services based on information from other services. The example added by Google, '*for example to make it easier to share things with people you know',* pertains to authenticated users and does not point out the fact that Google itself combines the data collected from all three types of users for its own purposes. The Dutch DPA once again refers here to the Article 29 Working Party's opinion on purpose limitation that: '(…) *each separate purpose should be specified in enough detail to be able to assess whether collection of personal data for this purpose complies with the law, and to establish what data protection safeguards to apply.'*[228] According to the legislative history of the Wbp as well, in the event of a primary purpose with sub-purposes or purposes existing alongside each other, each of the components is tested individually against Article 7 of the Wbp.[229]

In this context the Dutch DPA has distinguished four actual purposes, and ascertained that these are so vague or broad that during the collection process they cannot provide any framework against which it can be tested whether the data are necessary for that purpose or not. It follows from this that the purposes are not adequately defined in GPP2012 and the underlying pages to which GPP2012 makes reference.[230]
In its written view, Google writes that the Dutch DPA is suggesting that the purposes for which Google processes personal data are not adequately specific because of Google's reference in its Privacy Policy to possible future activities in which personal data could be processed (for example, an existing feature of its online service which is improved to increase user friendliness or to remedy a particular deficiency). According to Google, many of these future activities of Google will not serve any other purpose but have the same, explicitly specified, legitimate purpose (to provide the Google service). To the extent that information is processed for product development, Google writes, users are informed in the Privacy Policy that Google may use the information they provide to develop new products. Google states that it will

[227] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 79.
[228] Article 29 Working Party, Opinion 3/2013, p. 16.
[229] '*In the two other cases* [of sub-purposes and purposes existing alongside each other, added by the Dutch DPA] *the components of the purpose are each tested individually against Article 7 of this legislative proposal, whereby the underlying legal relationship is taken into account. This can occur particularly with businesses and institutions which provide diverse services and which can therefore also have diverse legal relationships with their clients.' Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 79.
[230] Article 29 Working Party, Opinion 3/2013 on purpose limitation, p. 19: '*It is important to emphasize that a failure to state, or accurately state the purpose or purposes for processing does not mean that the data controller can process personal data for any and all purposes at its discretion, or that it is free to determine the purposes based on its subjective expectations or unilateral interpretation of inconsistent information. (…) In such cases it will be necessary to reconstruct the purposes of the processing, keeping in mind the facts of the case.'*

always have to consider whether it is necessary to provide further information or obtain consent, from the perspective of proper data processing and in view of the reasonable expectations of users and the nature of the processing. However, according to Google, it would significantly limit the entire industry's innovative capacity if Google and other data controllers were required to provide more details on future product development.[231] Google claims that it cannot provide any detailed description of a future processing operation and that there is also no legal requirement for it to provide information on forms of data processing that do not actually take place.[232]

The response to this from the Dutch DPA is as follows. As stated, the four purposes investigated by the Dutch DPA in this report, which purposes are for the combining of data about and from several services, are inadequately specified in GPP2012 and the underlying pages to which GPP2012 makes reference. [233]

The Dutch DPA also does not assert that Google must provide detailed information on future product development, but ascertains that the purpose specification 'use information to improve services and develop new ones' is not specific enough to give users control over whether they want to allow Google to combine data with data about and from other services for this purpose and to assess whether the processing operations are lawful. The Dutch DPA is in no way insisting that Google must provide information about forms of data processing that do not actually take place. This is addressed in section 4.5 of this report.

The key conclusion from the Article 29 Working Party on the meaning of 'specific purposes' (the condition that purposes must be specific), is the following: '*Purposes must be specific. This means that - prior to, and in any event, no later than the time when the collection of personal data occurs - the purposes must be precisely and fully identified to determine what processing is and is not included within the specified purpose and to allow that compliance with the law can be assessed and data protection safeguards can be applied.*'[234]

In section 3.6 of this report the Dutch DPA ascertained that since the introduction of GPP2012, Google has not sought any new legal ground for the new data processing involving the combining of existing data from other services with new data (which are obtained via the new service). In none of these cases has Google informed the (authenticated and unauthenticated) users whether and how any data already collected would be combined with data about and from the new service. This is true in

[231] Google's written view, paragraphs 78-82. Google quotes from the Article 29 Working Party, Opinion 03/2013 on purpose limitation, p. 21, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[232] Google's written view, paragraph 82.
[233] Article 29 Working Party, Opinion 3/2013 on purpose limitation, p. 19: '*It is important to emphasize that a failure to state, or accurately state the purpose or purposes for processing does not mean that the data controller can process personal data for any and all purposes at its discretion, or that it is free to determine the purposes based on its subjective expectations or unilateral interpretation of inconsistent information. (…) In such cases it will be necessary to reconstruct the purposes of the processing, keeping in mind the facts of the case.*'
[234] Article 29 Working Party, Opinion 3/2013, p. 39.

particular for the integration of YouTube. Google has explained that as a result of the amendment of the privacy policy, it is able to share YouTube data with its other services, which was not possible previously because of the YouTube privacy policy.[235] Since that time Google has not added any clear information to the YouTube website about its identity as data controller, nor has it provided any specific information via YouTube about the consequences of the integration. The Dutch DPA understands from this that Google does not regard the combining of data about the use of YouTube as a new purpose and for that reason has not requested specific consent or provided the users with separate information. Because the purposes cited in GPP2012 and underlying pages are not specific enough to be able to foresee this, users could therefore be surprised by this integration if they discover that the search results are partly based on viewing behaviour, or that the personalised ads that they receive via third-party websites are partly based on the films they have viewed on YouTube.

Because the purpose specification in GPP2012 and Google's new stated objective for processing, 'to provide the Google service', are ambiguous and not specific enough, as far as these four purposes are concerned Google does not collect the data for specific purposes and is therefore acting in breach of Article 7 of the Wbp.

To the extent that Google takes the position that 'to provide the Google service' is the overarching primary purpose of the processing, it is the case that Google first mentions this in this written view, and not in GPP2012 or any notification to the Dutch DPA. In that case this purpose has been determined too late and/or explicitly described too late. After all, the reasoning of Article 7 of the Wbp is that the purpose specification must be determined in advance so that it can subsequently be tested (for example in the context of Article 9 of the Wbp) whether (further) processing (of the data already collected) takes place for incompatible purposes.

Whether Google satisfies the legal requirement that the examined actual purposes be legitimate is related to the assessment of the legal ground for the data processing that Google performs. This is assessed in section 4.6 of this report. It emerges from this that Google has no legal ground for the data processing operations for the four examined purposes. For this reason the personal data collected by Google for all three types of users for the four examined purposes are not collected for legitimate purposes and Google is also acting in breach of Article 7 of the Wbp on this point.

[235] Letter from Google to members of the US Congress on 30 January 2012: *'We had not updated YouTube's original privacy policy to include Google, with the result that Google could share information with YouTube, but not vice versa.'*

4.5 Obligation to provide information

Elaboration of the legal framework

Article 33(1) and (2) of the Wbp stipulates:
1. If personal data are to be obtained from a data subject, the data controller shall provide the data subject with the information referred to under (2) and (3) prior to obtaining said personal data, unless the data subject is already aware of this information.
2. The data controller shall inform the data subject of its identity and the purposes of the processing for which the data are intended.

Article 34(1) and (2) of the Wbp stipulates: *if personal data are obtained in a manner other than from the data subject, the data controller shall inform the data subject of its identity and the purposes of the processing, unless the data subject is already aware of this information:*
a. at the time that the data relating to him are recorded; or
b. if the data are to be provided to a third party, at the latest on the first occasion that said data are so provided.

The data controller must provide further information insofar as given the nature of the data, the circumstances under which they were obtained or the use that is made thereof, this is necessary to guarantee fair and careful processing with respect to the data subject, unless the data subject is already aware of this information (Article 33(3) and Article 34(3) of the Wbp).

Article 33 of the Wbp describes the situation in which the data are obtained from the data subject himself, for example when he is required to fill in details about himself on a form for a particular purpose.[236]

Article 34 of the Wbp provides for an obligation to provide information in situations where the personal data are obtained in a manner other than from the data subject himself, so without the data subject's involvement, either from third parties or through own observation, for example from the use of a network managed by the data controller.[237]

The obligation to provide (further) information described above does not apply when the personal data are obtained other than from the data subject if providing this information to the data subject proves impossible or requires disproportionate effort. In that case the data controller must record the origin of the data (Article 34(4) of the Wbp).

The obligation to provide (further) information also does not apply if the recording or provision is prescribed by or under the law. In that case the data controller must inform the data subject, at the latter's request, about the statutory requirement which has resulted in it having to record or provide the data relating to the data subject (Article 34(5) of the Wbp).

[236] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 149.
[237] Idem, p. 149-150.

These provisions elaborate the transparency principle and the 'fair processing' principle set down in Article 6 of the Wbp. The consequence of this is that breach of the obligation to provide information results in unlawful processing.[238]

The data controller's obligation to, on its own initiative, notify the data subject about the existence of the data processing is an important instrument in making data traffic transparent.[239] This enables the data subject to monitor how data about him are processed and to challenge in court certain forms of processing or unlawful conduct by the data controller.[240]

Articles 33 and 34 of the Wbp assume that the data subject does not have any obligation to investigate.[241] The legislative history reports in this respect: '*Article 6:228(2) of the Dutch Civil Code stipulates that a person cannot rely on error when concluding a contract if this is based on circumstances which, according to common opinion, should remain for the account of the party in error. The provision expresses the principle that when a contract is established, there is in general a balance between the one party's obligation to provide information and the other party's obligation to investigate. Which way the scale tips in a concrete case depends on circumstances such as the expertise of the parties involved and the knowledge that each party may presume the other to have. Such a balance also occurs in situations where there is no contract. (...) Under the regime of this legislative proposal, however, the data controller will only be permitted to consider itself relieved of its obligation to provide information if it knows that the data subject is aware. Articles 33 and 34 of this legislative proposal assume that the data subject does not have any obligation to investigate. This is based on the thinking that there is an inequality between the parties.*'[242]

Concurrence of Wbp and Tw

Article 11.7a(1) and (1a) of the Tw stipulates that any party that wishes to read or store data in a user's terminal equipment must provide the user with clear and comprehensive information in pursuance of the Wbp, and in any case information about the purposes for which it wishes to gain access to the relevant data or for which it wishes to store the data.

This Article is an implementation of Article 5(3) of Directive 2002/58/EC on privacy and electronic communication (e-Privacy Directive), as amended by the Civil Rights Directive 2009/136/EC. This directive provides for the protection of personal data and privacy for users of public electronic communication services.[243] The provisions from the e-Privacy Directive give further substance to particular general standards from the general Privacy Directive (for example, further limits/restrictions for permitted processing operations).[244]

[238] Idem, p. 149.
[239] Idem.
[240] Idem.
[241] Idem, p. 150.
[242] Idem.
[243] See Article 1(1) of the e-Privacy Directive; see also recitals 4, 8 and 12 of the e-Privacy Directive.
[244] See Article 1(2) and recital 12 of the e-Privacy Directive.

Assessment

4.5.1 Identity of the data controller

Google's service terms and conditions state that Google Inc. provides all of Google's services.[245] Google's logo is visible on virtually all its services, with the exception of YouTube. Because of the absence of a clear reference to Google as data controller on YouTube[246], authenticated and unauthenticated users are not informed adequately that Google can combine the data on the use of this service with data from other Google services such as Search or Maps (for the four examined purposes, namely to personalise requested services, personalise ads, product development and analytics).

Because this information about its identity as data controller in the Netherlands is absent, with respect to authenticated and unauthenticated users Google is acting in breach of Article 33 of the Wbp to the extent it receives the personal data directly from users or data subjects and in breach of Article 34 of the Wbp to the extent it receives the personal data in a manner other than directly from users or data subjects (the data on the use of YouTube).

4.5.2 Manner of providing information

The way in which Google provides data subjects with information about its privacy policy is not unequivocal and consistent. Essential information about the privacy policy (purposes of the data processing and types of data that are processed for those purposes) is spread across many different web pages and the designations used on these pages are not unequivocal. It is not logical that the information on the types of data that Google processes is to be found in 'Policy and Principles', divided under the headings 'Legal information' and 'Some technical details' and that this same information cannot be found in 'FAQ' in the section 'Legal information'. Google also no longer provides a central overview of the various sources containing more information on the privacy policy, such as some Help pages and FAQ or specific explanations per service.

In its written view Google contests that the information is provided in a fragmented way. It points to the fact that the homepage www.google.nl has a hyperlink to 'Privacy and terms', which links to a page with a clear overview of the key privacy-related documents such as the Privacy Policy, the 'FAQ' and the 'Good to Know' campaign. According to Google, the introduction of the new privacy policy is in fact a significant improvement compared to the 60 different privacy policies.[247]

The Dutch DPA notes that Google seems to contradict itself when on the one hand it points out that the 'Privacy and terms' page gives a clear overview of the key privacy-related documents and on the other hand accuses the Dutch DPA of ignoring the 'in-

[245] Google terms of service: *'The Services are provided by Google Inc. ("Google"), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.*' URL: https://www.google.nl/intl/nl/policies/terms/regional.html (last visited on 11 July 2013).
[246] The hyperlink to 'privacy' at the bottom of the YouTube homepage links directly to Google's privacy policy. The hyperlink to 'terms' (still) refers to a legal agreement with users of YouTube LLC, dated 9 June 2010. URL: https://www.youtube.com/t/terms.
[247] Google's written view, paragraph 39.

product notices' and Google support pages with detailed user guides. The Dutch DPA has factually ascertained that Google does not, via the 'Privacy and terms' page, unlock all the relevant information on the privacy policy, including answers to frequently asked questions and relevant explanations in the support centre. The Dutch DPA has also ascertained that the 'in-product notices' that Google provided to the CNIL provide virtually no information to users on Google's combining of data. The Dutch DPA has thoroughly searched in all the information that Google provides to users and developers on Google's use of (personal) data and documented each of these references in the footnotes of the report.

Given the enormous variety of services that Google offers, the way in which information is provided puts too onerous an obligation to investigate on all three types of data subjects. This is not only true for authenticated users, but also for unauthenticated users who have not created a Google account but who use Google's open services like Search, YouTube or Maps and for passive users who visit a website that allows Google to place and read DoubleClick or Analytics cookies. Because the information is provided in a fragmented way, on all sorts of web pages that often do not link directly to each other, the information provided is not clear, adequate and comprehensible. Because of this Google is acting in breach of the provisions of Articles 33 and 34 of the Wbp.

4.5.3 Further information on the combining of data

With regard to further information on the purposes for which data are combined, to the extent this is necessary in order to guarantee fair and careful processing with respect to the data subject in the sense of Articles 33 and 34 of the Wbp, the following applies.

The reasoning behind the obligation to provide information is, as stated, to enable the citizen to monitor how data about him are processed and to challenge in court certain forms of processing or unlawful conduct by the data controller.[248]

In terms of content, the formulations that Google uses in its (2,327-word) privacy policy are virtually never restrictive. The privacy policy contains examples or indications that a processing operation *is possible*. The (Dutch version of) GPP2012 contains twelve instances of the signal word '*bijvoorbeeld*' [for example], 24 instances of the signal word '*zoals*' [such as], 33 sentences with the (indefinite) verb '*kunnen*' [can/may], and eight instances of the adjective '*bepaalde*' [certain, particular] (in combination with 'data' or 'services' that are not specified further). Under the heading 'How we use the information we collect' there are a total of fifteen sentences. These contain four instances of the signal word '*zoals*' [such as], eight instances of the verb '*kunnen*' [can/may], three instances of the word '*bijvoorbeeld*' [for example] and one instance of the adjective '*bepaalde*' [certain, particular]. The following sentence is typical of the non-restrictive descriptions: '*We may combine personal information from a certain service with information, including personal information, from other Google services – for example to make it easier to share things with people you know* [underscore added by the Dutch DPA].'

[248] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 149.

In a general sense, the Dutch DPA points out that examples in a privacy statement can be very useful in making data subjects aware of specific data processing operations. In that case, however, the examples must give a representative picture of the impact of the data processing operation, so that data subjects are given the opportunity to exert control on the data processing and exercise their rights. The examples that Google uses are not adequately representative in that they only pertain to processing operations that intrude on the privacy of data subjects to a minor extent, such as the use of cookies to remember language preferences. By failing to give examples of processing operations using cookies which can intrude on privacy to a greater extent (such as the use of DoubleClick cookies to tailor ads on the more than two million websites and apps in the Google Display network), Google omits relevant information on the nature and scope of the data processing.

In GPP2012, Google writes as follows in relation to cookies:
'We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.'

The average user cannot gather from Google's cited purposes of improving the user experience and the overall quality of the services that Google can combine data from the contents of e-mail and documents with data that Google gathers on the use of other services, including geolocation services used on a smartphone with the Android operating system, to tailor services and to display targeted ads. Furthermore, from the last sentence quoted above the user could conclude that Google does not combine any data it obtains from the use of other services in order to tailor DoubleClick ads. But that assumption would be incorrect. In GPP2012, Google does not use the legal term 'personal data' [*persoonsgegevens*] but its own term 'personally identifiable information' [*persoonlijke gegevens*]. According to Google, these are only data that have been (deliberately) provided to Google by the user himself, such as name, e-mail address or invoicing information.

Google does not provide a complete overview of its different services and refused to provide one to the CNIL.[249] The specific product notices that Google sent to the CNIL (as discussed on pages 25-26 of this report) contain information on blocking certain content data provided by people themselves (such as film clips or profile information) for third parties, but no information on the combining of data by Google itself. To the extent that these product notices do contain information on the purposes of the data processing, these are descriptive examples and never an exhaustive description of the purpose of the processing.

Because there is no overview of services and no specific privacy notices for specific services, it is not adequately clear what data exactly Google combines for what purposes, and what the nature and scope is of Google's combining of data.

[249] Letters from Google dated 20 April 2012 and 21 June 2012, in answer to question 5.

In its written view, Google writes that its privacy policy is sufficiently specific.[250] According to Google, the purpose of a privacy policy is not to describe all the technical possibilities or what a data controller will not do, but it must describe, to an appropriate level of detail, what a data controller will in fact do.[251] According to Google, the repeated use of words like '*kan*' [can/may] in GPP2012 is unavoidable because Google will not collect the particular information in all cases. According to Google, such collection depends on whether the user is using a particular Google service, the relevance of the data for the specific service and whether the data are provided to Google. The last situation is not the case, for instance, if the user's browser does not accept cookies.[252] Google claims that this kind of wording furthermore takes future technological changes into account. A privacy policy that only uses unconditional wording does not take this reality into account, according to Google.[253]

The response to this from the Dutch DPA is as follows. A privacy policy does not need to explain in detail what data processing operations do not apply, but must give data subjects a clear picture of the envisioned data processing. The obligation to provide information is intended to ensure that, based on the information in the privacy policy and underlying pages, the average Internet user is able to estimate what types of personal data are processed for what purposes, what the consequences of these processing operations are and how he can exercise his rights. Specifically informing the data subjects therefore automatically means that the limits of the data processing must also be indicated. This means that Google can and must indeed clearly explain in its privacy policy the outlined circumstances in which it actually combines data for the four examined actual purposes. Google could and must clarify for each of the four examined purposes for the combining of data what personal data it combines for each purpose and outline the most important avenues by which it collects data, such as the Google account with Gmail, Drive, Google+ and Google Play and Google Music, open services like Search, Maps and YouTube, and finally, data that it collects via third-party websites.

Google can and must specify that it only collects certain data if a user (deliberately) uses a particular Google service (specifying whether it matters if a user is signed in or not) and explain that it sometimes does not collect certain data, for example if the user has set his browser not to accept (third-party) cookies.[254]

[250] Google's written view, heading 4.3: 'Google's Privacy Policy is adequately specific'.
[251] Google's written view, paragraph 38. See also paragraph 82: ' *For the rest, there is also no legal requirement to provide information on forms of data processing that do not actually take place.*'
[252] Google's written view, paragraph 38.
[253] Idem.
[254] See, for example, the Cookie and Privacy Policy of Albert Heijn (version of June 2012) on the point of layered information and the data that are processed with the use of the Anonymous Bonus Card in combination with various AH services. Dutch DPA, z2012-00068, Investigation into personal data processing by Albert Heijn B.V. in the context of the AH Bonus Card/Mijn Bonus advantage programme, November 2012, appendix 2, URL: http://www.cbpweb.nl/downloads_rapporten/rap_2012-ah-bonus-persoonsgegevens.pdf.

The dependency outlined by Google on whether data collection is 'relevant' for a specific service does not provide users with any footing in assessing whether certain data relating to them are processed and, if so, whether this processing is lawful. The average user cannot conclude from the formulations in GPP2012 when data are, in Google's view, relevant for the purposes for which data are combined investigated by the Dutch DPA. On the point of 'relevance', Google emphatically leaves all options open. Is the content of documents in Google Drive or an overview of YouTube clips viewed relevant for personalising advertisements, within Google (for instance via Gmail) or via third-party websites? Are directions called up via Maps relevant for personalising search results? The authenticated and unauthenticated users are not given any information on this. Are identifiers from and on mobile devices relevant for personalisingadvertisements on third-party websites? Even if passive users of Google services come in contact with Google's privacy policy, they cannot find any answers to these questions.

The fact that Google reportedly needs to use the word '*kan*' [can/may] so frequently in GPP2012 in order to take technological changes into account is, as reported above, not a valid argument. If, because of technological changes, such as the introduction of new services, Google wants to combine new types of personal data, for new purposes that data subjects could not reasonably expect, Google will have to take measures, by informing data subjects, for instance, or asking for consent for this new processing operation, especially with regard to data subjects (in all three capacities) on whom Google has already collected data.

In GPP2012 Google says that it asks for consent '*before using information for a purpose other than those that are set out in this Privacy Policy*'. In section 3.6 of this report, the Dutch DPA ascertained that this safeguard has not (yet) been applied in practice. From the investigation of the facts, it emerges that with the term 'consent', Google (wrongly) means the opportunity to opt out, as in the recent amendment of the terms of service for Google+ users which allows Google to use photos and data from Google+ profiles in advertisements. This misinterpretation of the term 'consent' is also evidenced by the way in which Google asks for 'consent' on its own websites and via third-party websites for the data processing related to the placement and reading of tracking cookies. The statement in GPP2012 about asking for consent is therefore misinformation, or is at least inadequately clear, on when there is a case of consent and/or of other purposes.

The lack of clear information is even worse for passive users. They do not even know that they are using Google services when they visit the websites of third parties who allow Google to place or read cookies on their terminal equipment, unless the website owner informs them about this. According to the April 2013 investigation that the Dutch DPA carried out into cookies on the 8,000 most visited websites in the Netherlands, more than 20% of the most visited websites in the Netherlands contain DoubleClick advertisements and more than 65% contain Analytics code. Website owners who use Google Analytics and/or Google DoubleClick are required by Article

11.7a of the Tw to notify visitors (and ask their consent) before placing and reading cookies (for more about this, see section 4.6.1 of this report).[255]

The lack of clarity on the purposes for which data are processed means that the data subjects are not adequately able to determine whether the purposes are legitimate and whether they want to make use of one or more of Google's services in exchange for allowing their personal data to be processed.

Because of the absence of clearly defined purposes for the data processing operations, Google is acting in breach of the provisions of Articles 33 and 34 of the Wbp, in conjunction with Article 6 of the Wbp, with respect to all three types of users for the four purposes for which data are combined and which are tested in this report.

4.5.4 Information on the types of personal data

In GPP2012 Google distinguishes two types of data: 'Information you give us' and 'Information we get from your use of our services.'

According to GPP2012 this second category covers device information, log information, location information, unique application numbers, local storage and cookies and anonymous identifiers. In response to the CNIL's questions on the exact types of data that Google collects and combines, Google created new sub-pages at the end of June 2013 with further information on location details, credit card data, unique device identifiers, biometric data and telephony.

The new information on the types of data is not restrictive and describes situations in which types of data *can* be used. The notices indicate that Google can tailor ads based on the user's visits to other websites in the Google content network, various types of cookies, unique device identifiers, anonymous identifiers on mobile devices, the IP address, and based on the model of the device used, the browser type or sensors. Google does not state and does not inform data subjects in what cases these data are combined. It cannot be concluded from the Google definition of unique device identifiers whether these are IMEIs (unique device numbers), MAC addresses, UUIDs or other identifiers. It also remains uncertain whether Google addresses sensors on smartphones other than the accelerometer mentioned.

In its written view, Google writes that the information it provides via its privacy policy contains sufficient details and gives users enough specific information on how Google uses their data in order to provide its online service.[256] In accordance with the Article 29 Working Party's wishes, Google drafted a policy that it claims is not formulated in an unnecessarily complex or legal manner, to the level of detail it considered appropriate for the target group (and which will not become quickly outdated because of technological developments). The privacy policy contains

[255] See the ACM's FAQ on the cookie provision (most recently updated on 5 July 2013), URL: https://www.acm.nl/nl/publicaties/publicatie/11643/Veelgestelde-vragen-over-de-nieuwe-cookiebepaling/

[256] Google's written view, paragraph 29.

hyperlinks which the interested user can use to find further information elsewhere.[257] According to Google, it is not functional to explicitly mention IMEIs, MAC addresses, UUID and accelerometers in the privacy policy since most users are not familiar with these terms.[258]

The Dutch DPA's response to this is as follows. The Dutch DPA is in no way arguing that Google's privacy policy should be very complicated, long, technical or legal in nature. The obligation to provide information is aimed at providing insight into the key properties and features of the service provision in a way that enables all types of users to make a conscious decision on whether to consent to the proposed data processing and the impact this has on their privacy.

If Google wishes to draft its privacy policy in accordance with the wishes of the Article 29 Working Party, this would be a layered policy, with the first layer containing the most important information for users, the second layer containing the details, for example via hyperlinks, and a possible third layer for all other relevant details.[259] The first layer must contain the core information which enables users to determine the impact that the processing operations will have on their privacy, and must therefore contain a comprehensible overview of the types of personal data that Google processes, and for what purposes. The user must be able to easily understand from those purposes what does and what does not happen with his data.[260] This information should not be limited to just the authenticated users, but must explicitly also be directed at unauthenticated and passive users.

The fact that a privacy policy must not become outdated too quickly because of technological developments is not a valid argument for providing too little information. If, because of technological changes, such as the introduction of new services, Google wants to combine new types of personal data, whether or not for new purposes, Google must in any event notify data subjects about that, in particular via its privacy policy. Although the law does not prescribe that Google must have an online privacy statement/privacy policy, in practice this kind of document is really the only way for it to comply (in a timely manner) with its obligation to provide information, given the fact that the communication between it and data subjects takes place exclusively electronically.
With regard to technical details such as IMEIs, MAC addresses, UUID and accelerometers, these are further technical details that are relevant for data subjects to determine what personal data are processed for what purposes, and for them to be

[257] Google's written view, paragraph 31.
[258] Google's written view, paragraph 32.
[259] Article 29 Working Party, Opinion 10/2004 on More Harmonised Information Provisions, p. 8-9, URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf
[260] Idem, '*This must offer individuals the core information required under Article 10 of the Directive namely, the identity of the controller and the purposes of processing - except when individuals are already aware -**and any additional information which in view of the particular circumstances of the case must be provided beforehand to ensure a fair processing.** In addition, a clear indication must be given as to how the individual can access additional information.*'

able to exercise their rights. Google can and must provide access to these data in a second level (via a single hyperlink) in its privacy policy, in relation to the specific purpose for which Google collects and processes these data.[261]

The same applies for the description of the use of location details. These are data of a sensitive nature. Google can use the content of search queries to determine an implicit (interest in a) location and can use GPS signals, device sensors, WiFi access points and IDs from radio towers to estimate the location.[262] Because Google does not otherwise delimit or explain the use of the location details, the average Internet user cannot determine the nature and scope of the data processing. Earlier investigation by the Dutch DPA in the context of the Street View service, for instance, indicated that Google has a database of MAC addresses of WiFi routers in the Netherlands and their estimated location.[263] Google does not mention this in its explanation on the use of location details. Based on the current explanation, Google does not rule out that it may combine these data with the geolocation data that it collects from smartphones with the Android operating system, for instance, in order to enrich the database with data on WiFi routers or personalise ads on the basis of (a profile of) movement patterns.

With regard to payment data, including credit card data, the explanation seems to contain a delineation of the purposes for which Google uses the data, namely to process payments and prevent fraud. The Google Wallet privacy policy explicitly states, however, that the general privacy policy applies, and that the payment data can therefore also be combined with data from all other Google services in order to personalise requested services, for product development and in order to display personalised ads.
The new explanations that Google gave at the end of June 2013 for a number of types of data fall short, therefore. They are not specific enough to enable the user to make a conscious decision to allow the data processing.

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 with respect to all three types of users.

[261] For the use of IMEI numbers, see for example the privacy statements from T-Mobile (URL: https://www.t-mobile.nl/Global/media/pdf/privacy-statement.pdf) and KPN (URL: http://www.kpn.com/privacy.htm).
[262] Google Policies and Principles, 'Types of location data used by Google' hyperlink, URL: http://www.google.com/intl/nl/policies/technologies/location-data/ (forensically recorded by the Dutch DPA on 1 July 2013).
[263] Dutch DPA z2010-00582, Definitive findings of the Dutch DPA investigation into the collection of WiFi data by Google with Street View cars, 27 December 2010, p. 26-27, URL: http://www.cbpweb.nl/downloads_rapporten/rap_2011_google.pdf.

4.6 Legal ground

Elaboration of the legal framework

In order to process personal data, one of the legal grounds (justifications) enumerated in Article 8 of the Wbp is required.

> Article 8, opening words and (a) (b) and (f) of the Wbp stipulates, insofar as is relevant to this investigation: *personal data may only be processed where:*
> *a. the data subject has unambiguously given his consent for the processing;*
> *b. the processing is necessary for the performance of a contract to which the data subject is party, or for actions to be carried out at the request of the data subject and which are necessary for the conclusion of a contract;*
> *f. the processing is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data are supplied, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail.*

Unambiguous consent

With regard to the legal ground of unambiguous consent (Article 8, opening words and (a) of the Wbp), the following applies.

There is only consent if it is 'freely given', 'specific' and 'informed' (Article 1, opening words and (i) of the Wbp). 'Freely given' means that the data subject must be able to exercise his will in freedom.[264] 'Specific' means that the expression of will must relate to a particular data processing operation or a limited category of data processing (no generally formulated authorisation).[265] 'Informed' means that the data subject must have the necessary information at his disposal in order to form an accurate judgement.[266]

Consent is only *unambiguous* if, for the data controller, all doubts have been ruled out as to whether the data subject has given his consent.[267] '*Unambiguous*' means that the data controller may not assume it has been granted consent just because the data subject has not remarked upon the data processing (or: 'consent' that is deemed to issue from the data subject's inaction or silence).[268]

In the legislative history of the Wbp, the following is noted with regard to this:

---

[264] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 65.
[265] Idem. In its opinion, the Article 29 Working Party commented with regard to this: *'Blanket consent without determination of the exact purposes does not meet the threshold. Rather than inserting the information in the general conditions of the contract, this calls for the use of specific consent clauses, separated from the general terms and conditions.* Article 29 Working Party, Opinion 15/2011 on the definition of 'consent' (July 2011), p. 40, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/ wp187_nl.pdf.
[266] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 65.
[267] Idem, p. 80.
[268] Idem, p. 66 and 67. Article 29 Working Party, Opinion 15/2011 on the definition of 'consent', p. 28 and 41.

'As example I cite general terms and conditions that apply to the conclusion of a contract. If such terms and conditions stipulate what data are processed for what purpose and by whom, this does not automatically mean that the data subject has unambiguously consented to this, merely because he has signed the particular contract.'[269]

In its opinion, the Article 29 Working Party also stated the following in relation to 'unambiguous consent':

'Consent based on an individual's inaction or silence would normally not constitute valid consent, especially in an on-line context. This is an issue that arises in particular with regard to the use of default settings which the data subject is required to modify in order to reject the processing. For example, this is the case with the use of pre-ticked boxes or Internet browser settings that are set by default to collect data.'[270]

If the consent does not satisfy the above requirements, it is invalid.[271]

With regard to the placement and reading of data on users' peripheral equipment, Article 11.7a of the Tw further limits/restricts, to some extent, the possible legal grounds as enumerated in Article 8 of the Wbp which may be eligible for personal data processing. Pursuant to the Tw, such operations are only permitted after prior consent from the users.

Article 11.7a of the Tw reads, to the extent relevant to this investigation:
1. Without prejudice to the provisions of the Personal Data Protection Act, any party that wishes to acquire access by means of an electronic communications network to data stored in a user's terminal equipment or that wishes to store data in the user's terminal equipment:
a. must provide the user with clear and complete information in accordance with the Personal Data Protection Act and in any case regarding the purposes for which such party wishes to acquire access to the data concerned or wishes to store data; and
b. must have acquired the user's consent for the action concerned.
An action as referred to in the opening words, which has the purpose of collecting, combining or analysing data on the user's or subscriber's use of various information society services for commercial, charitable or ideological purposes is presumed to constitute data processing as referred to in Article 1(b) of the Personal Data Protection Act.
(…)
3. The provisions in the first and second paragraphs do not apply insofar as it involves the technical storage of or access to data:
a. with the sole objective of carrying out the transmission of a communication over an electronic communications network; or

[269] *Proceedings I* 1999/2000, 34, p. 1632. Cf. also CJEU, 19 July 2012, case C-112/11 (ebookers.com), legal ground 16 and CJEU, 9 November 2010, case numbers C-92/09 and C-93/09.
[270] Article 29 Working Party, Opinion 15/2011 on the definition of 'consent', p. 41.
[271] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 67.

b. where such storage or access is strictly necessary to provide an information society service requested by the subscriber or user.

Consent from a user is defined in Article 11.1, opening words and (g) of the Tw and comprises consent that is 'freely given', 'specific' and 'informed' (Article 1, opening words and (i) of the Wbp).

Performance of a contract

With regard to the legal ground of performance of a contract (Article 8, opening words and (b) of the Wbp), the following applies.

Data processing is permitted if it is necessary in order to comply with contractual obligations.[272] The condition applies here that it must involve a contract to which the data subject is a party[273] and of which the data processing is a necessary consequence (that is: if the contract cannot be properly performed without the personal data).[274] The publisher of a newspaper may process its subscribers' personal data, for instance, because this is necessary in order to be able to deliver the newspaper[275] (delivery cannot take place without the particular data subject's name and address details). The processing cannot rely on this legal ground if the processing would simply be useful or would facilitate the performance of a contract, but is not really necessary since there is a way to perform the contract without the personal data (proportionality and subsidiarity test).[276] The legal ground is strictly limited to the data necessary for the performance of the contract.

In its judgment of 25 March 1983, the ECHR considered as follows in relation to the term 'necessary': *'(a) the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" (…).'*[277]

If supplementary, non-essential data are processed, this legal ground does not apply. In other words: there must be a justification for the processing *in the relationship with*

[272] Idem, p. 80.
[273] Idem. *'The underlying idea is that the data subject himself can, in principle, have a view on what processing operations he must expect and is able to objectively determine what processing operations are permissible in this context.'* Dutch DPA, 31 July 2001, z2001-0179.
[274] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 81.
[275] *Handleiding voor verwerkers van persoonsgegevens* [Manual for processors of personal data]. *Wet bescherming persoonsgegevens* [Personal Data Protection Act], Ministry of Justice, The Hague: 2002, p. 22.
[276] See also the Supreme Court, 8 September 2011, *LJN* BQ8097 on, *inter alia*, the proportionality and subsidiarity requirement for the legal grounds, as referred to in Article 8, opening words and (a) to (e) of the Wbp. The infringement of the interests of the data subject affected by the data processing may not be disproportionate in relation to the purpose to be served by the processing (proportionality) and the purpose for which the personal data are processed must not reasonably be able to be realised in a different way that is less detrimental for the data subject affected by the personal data processing (subsidiarity).
[277] ECHR, 25 March 1983, no. 97 (Silver & Others v. United Kingdom).

the specific individual data subject.[278] This means that the legal ground can only be applied if the data controller cannot properly perform the contract with this data subject without the data subject's specific, individual personal data.

Legitimate interests

With regard to the legal ground of being necessary for a legitimate interest (Article 8, opening words and (f) of the Wbp), the following applies.

A data processing operation is permissible if it is necessary in order to uphold the legitimate interests of the data controller (for example, so that it can perform its regular business activities[279]) or of a third party to whom the data are supplied, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail. This legal ground can be applied if the processing is necessary (proportionality test: the infringement of the interests of the data subject affected by the data processing may not be disproportionate in relation to the purpose to be served by the processing) and the purpose cannot be achieved otherwise or using less drastic means (subsidiarity).[280]

In supplement to this first consideration (necessary for a legitimate interest of the data controller), in which the interests of the data subject may have already been reviewed as part of an array of interests, there is also a second test.[281] This second test (the privacy test) demands a further consideration in which the data subject's interests are weighed up independently against the interest of the data controller. If the data subject's interest in protecting his own privacy outweighs the data controller's interest, the data controller must refrain from the data processing.[282]

Assessment

When asked by the CNIL about a legal ground for the combining of data, Google indicated that this legal ground depends on the type of product or service and can be found in Article 7(a), (b) or (f) of the Privacy Directive, i.e. Article 8, opening words and (a) (b) or (f) of the Wbp.[283] In its written view as well, Google confirms that to the extent the Wbp applies, it can appeal to several legal grounds in Article 8 of the Wbp. On which legal grounds Google can appeal in a concrete case depends in part on the nature of the data, the manner of processing and Google's relationship with the data subject, as well as the context of the processing in a broader sense.[284]

[278] Cf. *Parliamentary Documents II* 1998/99, 25 892, no. 6, p. 34: '*This means that as a rule, a justification for data processing must be identifiable in the individual person on whom data are being gathered.*'
[279] Idem, p. 86.
[280] Cf. the proportionality and subsidiarity test from Article 8 of the ECHR. *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 80. See also idem, p. 8 and idem, no. 92c, p. 6.
[281] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 87.
[282] Idem.
[283] Letter from Google to the CNIL dated 20 April 2012, answer to question 32.
[284] Google's written view, paragraph 58.

4.6.1 Consent

In section 3.3 of this report the Dutch DPA ascertained that Google uses various cookies to place and read data on computers and mobile devices of users in the Netherlands, on its own websites and via third-party websites. Pursuant to Article 11.7a of the Tw, Google must request informed, prior consent for this because the cookies are not exempt from the consent requirement.

In its written view, Google declares that with regard to its own websites it acts in accordance with the principles anchored in the Tw, e.g. by displaying a notification bar for Dutch users on www.google.com and www.youtube.com about the use of cookies and giving them the option to click through to 'Learn more'.[285] Where Google cookies placed and read via the websites of Google's partners are concerned, Google states that it has made contractual agreements that these partners will inform visitors and ask for their consent where this is required. [286]

Consent via Google's own websites (authenticated and unauthenticated users)

In section 3.3.1 of this report the Dutch DPA ascertained that Google already places and reads various cookies when its own websites Search, Maps and YouTube are loaded, before the user can choose to accept or refuse the cookies. This is also true of the additional Analytic cookies that Google places when a user clicks on the option 'Learn more'. This does not qualify as prior consent. Nor does Google satisfy the requirement that the consent must be informed. Although Google has, since mid-April 2013, displayed a pop-up screen on its own search result pages giving a hyperlink to 'more information', Google places and reads the cookies even before the user has had the chance to read this information. Clicking on a 'more information' button cannot be interpreted as giving consent since the visitor has only requested more information.[287] Google's working method on its own websites is therefore not compliant with the provisions of Article 11.7a of the Tw because these provisions require that visitors must give informed consent before cookies are placed and read.

For the record, the Dutch DPA points out that the exemptions from the obligation to provide information and the consent requirement for functional cookies, both contained in Article 11.7a of the Tw, do not apply to the PREF, NID and Analytic cookies (and the DoubleClick cookies on YouTube) that Google places and reads in order to register visits to its own websites. After all, the placement and reading of these cookies is not strictly necessary for transmission of the communication via Google's various websites (the websites also work without the cookies). The functionality of web statistics and advertisements also does not satisfy the

[285] Google's written view, paragraph 43.
[286] Google's written view, paragraphs 44 and 45.
[287] Cf. also the Article 29 Working Party, Working Document 02/2013 providing guidance on obtaining consent for cookies, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf, p. 5: *'Additionally, only a click to a "more information on cookies" link cannot be deemed consent, due to the fact that the user explicitly requested only for more information.'*

requirement that this be necessary for a service requested by the user (Article 11.7a(3)(b) of the Tw).[288]

Consent via third-party websites (all three types of users)

In section 3.3.2 of this report the Dutch DPA ascertained that Google and the website owners do not ask for any informed consent before placing and reading Analytic and DoubleClick cookies. Most of the cookies have already been placed before consent is asked for. This does not qualify as prior consent.

Pursuant to Article 11.7a of the Tw the placer/reader of the cookies must inform the visitor and obtain his consent. Google is the party that actually places and reads the DoubleClick and Analytic cookies via the websites of third parties. Google can outsource the provision of information and the obtaining of consent to these third parties, but Google will continue to bear the risk of the absence of informed consent. The Dutch DPA has ascertained that neither Google nor the third parties obtain consent.

Google and the website owners do not satisfy the requirement that the consent must be informed. Although Google requires the parties that purchase its Analytics and DoubleClick services to obey the law and inform website visitors about the collection of data[289], the Dutch DPA ascertained that the majority of the 50 most visited websites in the Netherlands do not comply with this requirement.

For this reason, the working method Google employs via third-party websites is also not compliant with the consent requirement contained in Article 11.7a of the Tw and the obligation to provide users with clear and complete information in accordance with the Wbp.

These cookies also do not fall under the exemptions to the obligation to provide information and the consent requirement which Article 11.7a of the Tw cites for functional cookies because the placement and reading of these cookies is not strictly necessary for transmission of the communication via third-party websites. The functionality of web statistics and advertisements also does not satisfy the requirement that this is necessary for a service requested by the user (Article 11.7a(3)(b) of the Tw).[290]

[288] The Dutch DPA has submitted the above application of the exemptions to the obligation to provide information and the consent requirement in Article 11.7a of the Tw to the ACM in the context of the Dutch DPA-OPTA cooperation protocol of the two regulators. The ACM agrees with the application of these exemptions presented in this report.

[289] It can be concluded from Google's answers to questions 56 and 57 in its letter dated 20 April 2012 that Google puts the full responsibility for compliance with privacy legislation on the website owners. In its letter dated 21 June 2012, Google reiterates: *'The Google Analytics terms of service oblige Google Analytics customers to comply with privacy laws, including an obligation to inform their website visitors about collection and use of the data.'*

[290] The Dutch DPA has submitted the above application of the exemptions to the obligation to provide information and the consent requirement in Article 11.7a of the Tw to the ACM in the context of the Dutch DPA-OPTA Co-operation Protocol of the two regulators. The ACM agrees with the application of these exemptions presented in this report.

In the present circumstances, the Analytic cookies via third-party websites also do not fall under the new exemption to the consent and information requirement if the draft legislative proposal amending Article 11.7a Tw becomes law, in the form it was presented in the Internet consultation up to 1 July 2013. If circumstances do not change, these cookies do not satisfy the requirement that the placement or reading of a cookie must have no or only minor consequences for the Internet user's privacy. This is addressed in more detail in section 4.6.4 of this report.

4.6.2 Unambiguous consent and tracking cookies

In section 4.3 of this report, the Dutch DPA ascertained that the PREF and NID cookies that Google places on its own websites are tracking cookies. The same is true of the DoubleClick cookies that YouTube places and reads. The DoubleClick cookies that Google places and reads via third-party websites are also tracking cookies. If, in accordance with its privacy policy, Google combines the Analytics data with data on DoubleClick cookies for retargeting purposes[291] and with data on social media use (Social Analytics), these are also tracking cookies.

The tracking cookies that Google places and reads via its own websites and via third-party websites are used to record data on visits to multiple websites. That is why this involves the processing of personal data (see sections 4.2.1 and 4.2.2 of this report). Article 11.7a of the Tw does not provide any legal ground for the processing of personal data. That is why Google must not only satisfy the provisions of Article 11.7a of the Tw, it must also have a legal ground for data processing for the actual purposes investigated in this report, i.e. the personalising of requested services, product development, the display of personalised ads and web analytics, as stipulated in Article 8 of the Wbp.

In view of the concurrence with Article 11.7a of the Tw[292] and in view of the European legislator's intention to provide the same level of protection under both statutory standards and the overlap of the definitions of consent and unambiguous consent, it seems obvious to assume, in the context of the personal data processing associated with the tracking cookies (including the processing resulting from it), that there is a requirement for unambiguous consent.[293]

[291] *The Google Analytics Tracking Code also reads the double-click cookie to inform Google Analytics for Display Advertisers'.* Source: Google ' How Does Google Analytics Collect Data?', URL: https://developers.google.com/analytics/resources/concepts/gaConceptsTrackingOverview?hl=en#howAnalyticsGetsData.

[292] See for example *Parliamentary Documents II* 2010/2011, 32 549, no. 39, p. 2. *'Aside from the consent requirement for the placing and reading of cookies in Article 11.7a of the Tw, the requirements in the Wbp must also always be satisfied if personal data are processed with or by means of the placement or reading of cookies. This means that in those cases based on Article 8 of the Wbp, "unambiguous" consent is required (...).'*

[293] In the same sense, see *T&C Telecommunicatierecht* [Text & Commentary on Telecommunications Law], comments on Article 11.7a of the Tw, note 3.

The legislative history does indicate that there could be other legal grounds[294], such as Article 8, opening words and (f) of the Wbp, if the data processing is necessary to uphold a legitimate interest, provided the data subject's interest in protecting his own privacy does not prevail. With tracking cookies, however, it is not considered plausible that the legitimate interest of the party that processes the data prevails over the individual's right to protection of privacy. *'For this reason, the "unambiguous consent" of the data subject will generally be required on grounds of the Wbp.'*[295]

To the extent that the combining of personal data is related to tracking cookies, Google can therefore only rely on the legal ground that it has obtained unambiguous consent.

As stated, there is only consent if the data subject expresses his will freely, specifically and on an informed basis (Article 1, opening words and (i) of the Wbp) by which the data subject accepts that personal data relating to him will be processed. The difference between 'consent' and 'unambiguous consent' is that the data controller must have no doubt whatsoever that the data subject has granted his consent.

Google may well agree with third parties that they must obtain the required unambiguous consent for it, but Google continues to bear the risk as data controller for the data processing. In section 3.3.2 of this report the Dutch DPA ascertained that via the 50 most visited websites in the Netherlands, where these websites place DoubleClick and Analytic cookies, Google does not obtain consent to combine, for the actual four purposes investigated in this report, the personal data it obtains. To the extent that Google indicates in its written view that it does not have any indications that these third parties do not obtain consent, the following applies. The legislative history shows that a data controller must actively verify whether unambiguous consent has been obtained. '*There is a shift of the burden of proof towards the data controller: if there is any doubt about whether the data subject has granted his consent, the data controller must verify whether he can correctly assume that the data subject has consented.*'[296]

With regard to the aspect 'unambiguous' in Article 8, opening words and (a) of the Wbp, the Dutch DPA points out the following. It is not automatically clear or obvious to the average Internet user when he visits a website with DoubleClick cookies that an

[294] See for example *Parliamentary Documents I* 2011/12, 32 549, E, p. 5-6. *'Contrary to what several members assume, the fact that these operations fall under the Wbp does not necessarily mean that they require unambiguous consent. Besides unambiguous consent from the data subject, Article 8 of the Wbp cites another five justifications.'* See also p. 7 '(…) *if none of the other justifications from Article 8 of the Wbp applies, unambiguous consent from the user must be a requirement,'* and p. 11-12: '(...) *have therefore obtained unambiguous consent or rely on a different justification from Article 8 Wbp.' 'Upholding the legitimate interests of the data controller can be a justification for the processing of personal data, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail. It is not plausible however that this will easily be the case with the use of tracking cookies. For this reason, the "unambiguous consent" of the data subject will generally be required on grounds of the Wbp.'* Notes to Draft legislative proposal with explanation concerning Article 11.7a of the Telecommunications Act (cookie provision), p. 15. URL: http://internetconsultatie.nl/cookiebepaling.

[295] Idem.

[296] *Parliamentary Documents II* 1997/98, 25 892, no. 3, p. 66-67.

option to (partially) refuse cookies is hidden behind the 'more information' button or behind the 'Ads (i)' icon at the top right of DoubleClick advertisements. Although the user can prevent the display of personalised ads via Google's Ad Settings, this does not enable the particular user to refuse the placement and reading of cookies and therefore also does not enable him to refuse the related processing of personal data. Consequently there is no clear choice for the particular website visitors to grant or refuse their consent for a proposed data processing operation. If there is to be unambiguous consent, it is important that there be no doubt about the question of whether the visitor has granted consent.[297]

The information field about cookies that Google introduced on its Search pages at the end of June 2013 contains three options: Clicking on OK, clicking through or ' More information'. If the user clicks on 'More information', he finds information on how Google uses cookies and hyperlinks to more information on the different types of cookies Google may use for, among other things, personalising search results, displaying personalised ads and Google Analytics and general information on managing cookies in browsers. This page contains no option for refusing the different types of cookies (via Google itself).
The use of the term 'expression of will' implies an action by the data subject (in other words, consent and not an opt-out). Google may not conclude that the data subject consents to this data processing simply because the data subject has not opted out or because the data subject has not utilised the option to refuse cookies by adjusting his browser settings. Even aside from the fact that Google already places cookies at the moment its various websites load, and places additional cookies at the moment the visitor clicks on 'More information', the current 'More information' page does not provide the possibility of obtaining (unambiguous) consent.

Only after clicking through five times from the information field on the Search pages can a user arrive at a menu where he can refuse the advertising cookies from Google.[298] After clicking twice, at the bottom of the page, the user will also find short instructions for users of mobile devices to stop Google from using anonymous identifiers on devices running the Android or iOS operating system for advertising purposes. These instructions are insufficient, however, to prevent Google from displaying personalised ads on mobile devices using cookies.

There is no situation of unambiguous consent for the data processing operations related to tracking cookies because Google does not provide visitors to its own websites and to third-party websites with a clear choice between consenting to the placement of (certain types of) cookies and refusing the cookies.

[297] See also the Notes to Draft legislative proposal with explanation concerning Article 11.7a of the Telecommunications Act (cookie provision), p. 8.
[298] By clicking on 'More information', 'How Google uses cookies', 'How Google uses cookies in advertising', 'Ads settings' and 'Opt out') (twice, once for tailored ads on Google and once for tailored ads across the web).

Unambiguous consent and terms of service

In its written view, Google writes that it obtains consent from authenticated users by virtue of their acceptance of the Terms of Service and the Privacy Policy by checking a tick box; for unauthenticated users this acceptance follows from the fact that they continue to use the website – which continued use constitutes acceptance according to Google's Terms of Service.

The legal framework at the beginning of section 4.6 of this report, under the heading 'Consent', indicates that unambiguous consent cannot be obtained through inclusion in general terms and conditions.

> *'As example I cite general terms and conditions that apply to the conclusion of a contract. If such terms and conditions stipulate what data are processed for what purpose and by whom, this does not automatically mean that the data subject has unambiguously consented to this, merely because he has signed the particular contract.'*[299]

This legal framework also highlights the fact that 'unambiguous' means that the data controller may not assume it has been granted consent just because the data subject has not made any remarks on the data processing (or: 'consent' that is deemed to issue from the data subject's inaction or silence).

Google's default setting is that users grant consent and it offers, at most, partial possibilities for opting out. In the event of product development, no possibility of opting out is available whatsoever. With regard to the personalising of ads, a data subject can only object to the display of these ads, but cannot object to the underlying data processing operations by Google without drastic loss of functionality (discarding cookies per session or fully blocking cookies in the browser).

The fact that it offers (partial) opt-out possibilities shows that Google assumes tacit consent from unauthenticated users for the use of data from one service (YouTube or Maps) to personalise the other service (Search) and for the combining of data from the open services for the display of personalised advertisements elsewhere on the Internet. In relation to authenticated users, Google also assumes tacit consent for the use of content from services like e-mails sent and received in Gmail and the content of documents on Drive to personalise advertisements and for the combining of data from all these services for the personalisation of advertisements elsewhere on the Internet.

Failure to comment (in this case, failing to use the limited opt-out options) does not result in legally valid consent.

[299] *Proceedings I* 1999/2000, 34, p. 1632. Cf. also CJEU, 19 July 2012, case C-112/11 (ebookers.com), legal ground 16 and CJEU, 9 November 2010, case numbers C-92/09 and C-93/09.

Unambiguous consent and information

Finally, unambiguous consent requires the information to be specific and the data subject to be informed, in the sense of Article 1, opening words and (i) of the Wbp. As the Dutch DPA ascertained in section 4.5 of this report, Google does not adequately inform its three types of users about the combining of personal data from different services, with or without the aid of cookies.

Google does not satisfy the criterion 'informed'. The different purposes for which data are combined are not fully described, or are at least not described clearly enough, in GPP2012 and the underlying pages to which GPP2012 makes reference. As explained earlier in this report, in the assessment of the obligation to provide information, because of this lack of information, data subjects cannot estimate the nature and scope of the data processing, for what purposes Google combines personal data relating to them, and to what extent tracking cookies play a role in this. Furthermore, Google hardly touches on the use of cookies to combine data for purposes other than the display of personalised ads. Google states: *'We use cookies for many purposes. We use them, for example (...).'* This does not make it clear that Google may also use the data for the purposes of personalising requested services, product development and website analytics.

Google also does not satisfy the criterion of 'specific' because it does not ask for consent for the various data processing operations for the four actual purposes investigated. Google only offers options (spread out in several places) for opting out of the display of personalised ads and points out the possibility of setting one's browser to refuse all cookies. It cannot be concluded from the underlying information what precise data are processed (and combined) and for what purposes. The descriptions used are not specific enough because one cannot conclude from these that Google places and reads at least two types of permanent cookies with unique identifiers and combines these with data on visits to multiple websites. For authenticated and unauthenticated users Google may combine these data with data from all other services which these data subjects use, including new services like Google Music, which were introduced after the introduction of the privacy policy. As a consequence of this, Google cannot obtain legally valid, specific consent from these users for data processing for the data-combining purposes investigated in this report. The fact that YouTube is not recognisable as a Google service also plays a role in this. Consequently the information is not adequately 'specific' and 'informed' in the sense of Article 1, opening words and (i) of the Wbp.

In summary, Google does not provide data subjects with a simple action by which they can accept or refuse the various types of tracking cookies. That is why there is no unambiguous consent. Although unambiguous consent can also be obtained from an active action, this is only the case if the user has been (freely) able to make a (specific and informed) decision either to consent or refuse, and that is not the case.[300] Nor does

[300] Notes to Draft legislative proposal with explanation concerning Article 11.7a of the Telecommunications Act (cookie provision), p. 12: *'If there is to be unambiguous consent, it is important that there be no doubt about the question of whether the Internet user has granted consent. This means that it must be clear that the Internet user had a choice to either consent or refuse.'*

Google obtain unambiguous consent by virtue of acceptance of its Terms of Service or the continued use of its open services. Google also does not obtain unambiguous consent for the data processing operations because the specific information required is missing. This applies for all three types of users. After all, even for data subjects who register with a Google account the information is not adequately specific and defined to enable them to form a picture of how their personal data are processed.

4.6.3 Necessity for performance of contract

In its written view, Google writes that the Terms of Service create a contractual relationship with all users of Google's services, irrespective of whether they are authenticated users or not. For this reason, Google says that it also relies on Article 8(b) of the Wbp. As an example of a processing operation that is necessary for the performance of a contract with the data subject, Google cites the processing of credit card details in order to process an online order placed by a user of Google Play.[301]

In sections 3.3.1 and 3.3.2 of this report, the Dutch DPA ascertained that Google often uses tracking cookies for data processing when combining personal data for the four examined purposes and that unambiguous consent is required for the data processing associated with and arising from this. For this reason alone, therefore, claiming a legal ground pursuant to Article 8, opening words and (f) of the Wbp cannot succeed.

Passive users

In contract law[302] a contract is established by the acceptance of an offer (according to Google: the Terms of Service, which contain a link to the Privacy Policy). The offer must be expressed and contain all essential elements of the contract to be concluded. Passive users in the Netherlands, in other words visitors to websites that use Google's (advertising) services, do not receive any proposal from Google to enter into a contract, electronically or otherwise. So they can hardly be said to have accepted an offer (since they have not even received one). Passive users will in most cases not even be aware that they have encountered or will encounter Google cookies when using third-party websites. The Terms of Service therefore certainly do not give rise to a contractual relationship with the passive users.

Unauthenticated users

The legal ground on which Google relies, Article 8, opening words and (b) of the Wbp, can apply with regard to unauthenticated users if a data processing operation is necessary for the performance of a contract to which the data subject is a party. Without prejudice to the question of whether a valid, inviolable contract can even be established in an online environment purely by the fact of visiting the Search, Maps or YouTube website, the key question here is whether the processing of personal data is necessary for the performance of the contract. Only in that case can Google rely on Article 8, opening words and (b) of the Wbp. The legislative history shows that the

[301] Google's written view, paragraphs 64-66.
[302] See for example Article 6:217 of the Dutch Civil Code (BW).

criterion of necessity explicitly refers to Article 8(2) of the ECHR and subsequent case law.[303]

To be able to rely on a legal ground pursuant to Article 8, opening words and (b) of the Wbp, the processing operations must therefore be necessary in order to provide the service. The fact that someone uses Search, Maps or YouTube as an unauthenticated user does not make it necessary to use these data in order to display personalised ads to that data subject elsewhere on the Internet (via websites that use Google advertisements) or to personalise search results for that data subject based on behaviour in the other open services. The placement and reading of the PREF and NID cookies on all websites in the Google domain (and DoubleClick cookies on YouTube) for these purposes is not necessary in order for Google to provide services to unauthenticated users.

Authenticated users
Regardless of any contractual agreement, it is also not proportionate, with regard to authenticated users, to combine data from the content of information that these users provide to Google, such as e-mail and app purchasing behaviour, in order to tailor search results or to combine data on and from the use of various Google services with data on visits to third-party websites in order to tailor advertisements.

As Google itself admits in its written view, it deliberately uses the words '*kan*' [can/may] and '*mogelijk*' [possible/possibly] in its privacy policy so that it does not – unintentionally and adversely – become contractually obligated to the data subject to use (combine) the data in a particular manner.[304] The combining of personal data is therefore not necessary in order to comply with a contractual obligation (just as this is not the case for unauthenticated users).

The same lack of necessity applies with regard to all three types of users for the other two purposes for which data are combined (product development and website analytics). No justification for these processing operations exists in the relationship with the specific individual data subjects (or any agreement entered into with them). The combining of data on and from multiple services for these purposes is more aimed at serving Google's general business interest, specifically: to obtain information on the use of its own services and record and analyse visits to third-party websites (including advertisements) so that it can improve the quality of its services and develop new services based on data already collected.

[303] *Parliamentary Documents II* 1997/98, 25 892, no. 6, p. 33. '*In this context the term "necessary" originates from Article 8(2) of the ECHR. In the original Dutch translation of the ECHR in the Treaty Series of 1951 (154), this term was translated with "*nodig*" [needed]. In the light of the subsequent case law of the European Court of Human Rights (ECHR), this term was translated into the Dutch as "*noodzakelijk*" [necessary] in the new translation in 1990 (Treaty Series 156). The terms related to this in European and Dutch case law, including "proportionality" and "subsidiarity", would not be done justice to as clearly if a return were now made to the old term "*nodig*" [needed].*'
[304] Google's written view, paragraph 38.

There are no legal grounds pursuant to Article 8, opening words and (b), therefore, for the data processing operations investigated in this report, i.e. the combining of data for the purposes of personalising requested services, product development, personalised ads and website analytics, with respect to any of the three types of users.

Google itself cites the processing of credit card details for purchases via Google Play as an example of the legal ground of necessity for performance of a contract. A legal ground for this specific data processing operation for authenticated users may indeed be found in Article 8, opening words and (b) of the Wbp, as could be the case for the (necessary) processing of data via Google Wallet in order to facilitate payments, and the creation of a Google account and/or e-mail address in order to be able to perform particular, specific processing operations. These two examples only pertain to the processing of personal data within a single service, however. They do not relate to the four examined actual purposes, for which Google combines data from and about multiple services, and therefore do not fall within the scope of this investigation.

4.6.4 Necessity for legitimate interests

With regard to Google's claim to have a legal ground pursuant to Article 8, opening words and (f) of the Wbp for the combining of data for the four purposes investigated in this report, the following applies.[305]

In sections 3.3.1 and 3.3.2 of this report, the Dutch DPA ascertained that Google often uses tracking cookies for data processing when combining personal data for the four purposes under investigation and that unambiguous consent is required for the data processing associated with and arising from this. Therefore, for this reason alone, claiming a legal ground pursuant to Article 8, opening words and (f) of the Wbp cannot succeed.

To the extent Google nonetheless claims a legal ground pursuant to Article 8, opening words and (f) of the Wbp for the examined data processing operations (the combining of data from and about multiple services), the following applies.

It is stated first and foremost that data controllers can have legitimate interests in developing new services on the Internet for which there is demand. In accordance with Article 8, opening words and (f) of the Wbp, the data controller must take into account the impact these services will have on the individual privacy of the data subjects. The data controller must build in safeguards to prevent any disproportionate disadvantage. Careful data processing requires that data subjects be actively informed about the recording of personal data relating to them and the specific purposes for which these data are collected and processed.

The way in which Google may combine all sorts of data from various services, according to GPP2012, does not adequately demonstrate that a proportionate weighing of interests has taken place (proportionality principle). It must also be taken into account here that if the data controller's legitimate interest can be served in some

[305] Google's written view, paragraph 67.

other way or by less drastic means, the data processing is not permitted (subsidiarity principle).

Google's necessity to collect (a limited set of) data on the use of its services and (further) process these data does not automatically entail a necessity to subsequently also combine the data thus obtained for the four purposes investigated in this report. As far as the combining of data from and about multiple services for product development purposes is concerned, Google has not demonstrated that it is necessary to use personal data for this, and if that is indeed the case, why a less infringing method cannot suffice, such as the use of test panels of users who have consented to this data processing. This involves the large-scale, covert collection of sensitive personal data (surfing behaviour) via cookies and the processing of those data. That is why the processing operations for this purpose have major consequences for the individual privacy of the data subjects.

With regard to the combining of data in order to display personalised ads, Google does have a legitimate interest in basing its business model on advertising revenue, but Google must comply with the requirements of proportionality and subsidiarity. Monitoring a user's behaviour across multiple websites and treating the data subject differently on the basis of that (with personalised ads) is a major infringement of the data subject's individual privacy.

Pursuant to the Wbp, the data controller has the duty to demonstrate the necessity of the data processing.[306] If Google were to demonstrate the necessity of specific data processing operations for specific purposes, Google must make a second, independent consideration on whether its legitimate interest outweighs the data subject's right to protection of his individual privacy,

In this second privacy test, the degree (seriousness) of infringement of the data subject's privacy plays an essential role, as do safeguards such as transparency and the existence of effective opt-out options for data subjects.

Google's combining of data, among other ways by using tracking cookies, from multiple services and third-party websites for the purpose of displaying personalised ads, personalising services, product development and analytics constitutes a major intrusion into the privacy of the users involved, for all three types of data subjects.

Impact for authenticated users
According to GPP2012 Google may combine the personal data of authenticated users with data on and from all other Google services. Google uses (tracking) cookies to record the use of its open services (Search, YouTube and Maps).

[306] *Parliamentary Documents II* 1998/99, 25 892, no. 13, p. 6: *'For the rest, we point out that just having a legitimate interest is not sufficient. According to Article 8(f) data processing can only be permitted if it is also "necessary" with the particular interest in mind. The data controller has the duty to demonstrate the necessity of the data processing.'*

In some cases, the combining of data may be obvious, like the display of Gmail contact details in the agenda, but in other cases, especially when the contents of documents are involved and for example a Google+ profile, location details, calling details, payment data and search queries, the processing can be a major infringement of the data subject's right to protection of privacy. Payment information and location details, for instance, are data of a sensitive nature, while the contents of e-mail and documents are confidential communication. What is more, Google offers highly diverse services which serve entirely different purposes from the point of view of users (such as searching, sending e-mails, viewing videos, buying apps). Finally, Google also combines these data with data on visits to many third-party websites in order to be able to display personalised ads or tailor services such as Search. The recording of visits to multiple third-party websites results in a sizeable collection of sensitive personal data that can provide information on people's behaviour on the Internet.

Impact for unauthenticated users
Google uses (tracking) cookies to record the use of its open services (Search, YouTube and Maps). Using these cookies Google can combine many types of data on the use of Google services with data on visits to third-party websites, in order to be able to display personalised ads or tailor services such as Search and YouTube. Just as for authenticated users, the recording of visits to multiple third-party websites results in a sizeable collection of sensitive personal data that can provide information on people's behaviour on the Internet. These data affect the confidential communication. With these, according to GPP2012 Google may combine data of a sensitive nature, such as location details (whether directly obtained or deduced).

Impact for passive users
It is not likely that passive users of Google services (the visitors to websites that allow DoubleClick or Analytic cookies to be placed and read) will come in contact with the Google privacy policy. They have not chosen to use Google's services but their website visit is nonetheless recorded by Google (in part, to the extent Google cookies are present on those websites). The data on users' visits to websites that Google collects and can combine for the purposes of displaying personalised ads, website analytics and product development are not necessary for the data subjects and website owners in order to enable the visit to the website. The data processing is at the expense of the right to protection of privacy of the passive users involved. Google's working method makes it almost impossible for a passive user to avoid having his personal data processed by Google.

The processing operations result in different treatment of all three types of data subjects when they are shown personalised ads.

In addition, Google has failed to put adequate safeguards in place to ensure that the combining of data is strictly limited to legitimate purposes and that the data subject's right to protection of individual privacy prevails.

With regard to Analytic cookies that are not tracking cookies, the Dutch DPA ascertained and verified with Google[307] during the investigation that Google was not offering data processing contracts to customers of Google Analytics services in the Netherlands (at least prior to 7 November 2013).

Because there are no such data processing contracts, Google may, according to GPP2012, combine the data it collects via its Analytics service with all sorts of other data from and on the use of all other Google services.

Even if the draft legislative proposal amending Article 11.7a Tw becomes law, in the form it was submitted for Internet consultation until 1 July 2013, these cookies do not – provided circumstances do not change – satisfy the requirement that the placement or reading of a cookie must have no or only minor consequences for the Internet user's privacy.[308] This is because Google does not exclude further use of the data by Google itself for its own purposes and the processing of these data therefore have more than minor consequences for the privacy of the Internet user to whom the data relate.

In early October 2013 the Dutch DPA learned from media reports that Google now intends to offer customers of the Analytics service in Europe a data processing contract.[309] In the absence of an official notification from Google to the Dutch DPA that Google will be offering Dutch website owners a data processing contract for Analytics, the status of this document is not sufficiently established and the Dutch DPA cannot give any opinion on this. It is possible that by concluding a data processing contract with Google for the use of Analytics, responsible website owners could rely on the new exemption to be set down in the Tw in relation to the consent requirement for cookies, but in that case the data processing contract must satisfy the statutory requirements. This means that the contract must in any event satisfy the requirements of Article 14 in conjunction with Article 12 of the Wbp. The starting point of a data processing contract is that the data controller (in this case, the website owner) itself

[307] The Dutch DPA spoke to representatives of Google Netherlands about this by telephone on 11 February 2013.

[308] On 20 May 2013 a draft legislative proposal amending Article 11.7a Tw was submitted for public consultation. See: http://www.internetconsultatie.nl/cookiebepaling (the consultation ended on 1 July 2013). The proposed amendment does away with the requirement to inform and ask consent if the placement or reading of a cookie provides information on the quality or effectiveness of an information society service provided, as long as this has no or only minor consequences for the Internet user's individual privacy. According to this draft legislative proposal, this includes analytic cookies, provided the company that shares its usage data from analytic cookies with a third party makes clear agreements in a (processing) contract with the third party that the third party will also not use the information in a way that has more than minor consequences for the privacy of the Internet user to whom the data pertain. Notes to Draft legislative proposal for the Internet consultation, p. 8.

[309] URL: http://www.google.com/analytics/terms/dpa/dataprocessingamendment_20130906.html, quoted in Webwereld, 'Google past na privacydruk Analytics in heel Europa aan', [Under privacy pressure Google amends Analytics throughout Europe] 7 October 2013, URL: http://webwereld.nl/beveiliging/79561-google-past-na-privacydruk-analytics-in-heel-europa-aan (URLs last visited on 29 October 2013).

must decide what types of data it processes, for how long and by what means. In order to be eligible for the new exemption, the Dutch DPA feels it is important that the contract must stipulate that as processor of the data, Google may only use the data in order to keep track of statistics on website use for the website owner and may not combine the data with other data for its (Google's) own purposes. This specifically applies also for the possibility of combining Analytic cookies with DoubleClick cookies and Social Analytics (the interaction of authenticated users with the +1 buttons), as well as with unique device identifiers of mobile devices or other methods for uniquely identifying individual users when they visit multiple websites. Google's potential role as data processor falls outside the scope of this investigation.
A crucial safeguard is transparency, to ensure that data subjects can exercise their rights, such as the right to revoke consent. This transparency is lacking.

In section 4.5 of this report, the Dutch DPA ascertained that Google does not inform the various groups of data subjects sufficiently and specifically enough about the key elements of the data processing, which consist of combining data from and about multiple services (the types of data and the purposes). Data subjects cannot conclude from GPP2012 and the underlying pages what actually happens with their personal data. It is not clear, or not sufficiently clear, what personal data are combined with each other and for what purposes.

In its written view Google writes that the fundamental rights and freedoms of data subjects do not outweigh [Google's legitimate interest, added by the Dutch DPA] because Google offers tools with which users can exercise their rights and because Google provides users detailed information.[310] Google cites as example the personalisation of search results for authenticated users based on the particular user's search history.[311] The user can turn off, pause or delete his search history in this process, or choose the incognito browsing mode in Chrome.[312]

The Dutch DPA's response to this is as follows. If Google did actually provide users with detailed information on the data processing operations which involve the combining of data from a number of its own services with data on surfing behaviour via third-party websites, this would in and of itself be an important safeguard in ensuring that the data subject's right to protection of privacy does not prevail over Google's legitimate interest in processing the data. The same applies for offering tools which users can use to exercise their rights. However, even with these safeguards, Google cannot claim a legal ground pursuant to Article 8(f) of the Wbp for the four examined purposes because the only possible legal ground for using personal data obtained with tracking cookies is unambiguous consent, and alternatively, the examined processing operations do not satisfy the requirements of proportionality and subsidiarity.

In response to Google's view that it offers a range of opt-out tools, the Dutch DPA nonetheless conducted a more in-depth investigation into the opt-out possibilities for

[310] Google's written view, paragraph 68.
[311] Google's written view, paragraph 69.
[312] Google's written view, paragraph 70.

the different types of data subjects. In section 3.7 of this report the Dutch DPA ascertained that Google offers the different types of data subjects different types of partial opt-out possibilities, but not for all the purposes investigated in this report (not for product development). Furthermore, these opt-out options do not in all cases result in termination of the data processing (for instance, the opt-out for the display of personalised ads).

Opt-out options for authenticated users
With regard to the personalisation of requested services, authenticated users can object in each service, such as Search and YouTube, but they cannot object to Google combining data from and about their use of other services with those services. The opt-out options that Google makes available here are labour-intensive, do not result in all cases in the actual deletion of the data and furthermore result in a loss of functionality.

Opt-out options for unauthenticated users
In section 3.5 of this report, the Dutch DPA ascertained that Google does not adequately inform unauthenticated users about the possibility of opting out of personalised search results. Unauthenticated users cannot object to the personalisation of results in YouTube and Maps other than by refusing cookies in the browser (with the corresponding loss of functionality).

Opt-out options for passive users
In section 3.5 of this report, the Dutch DPA ascertained that the possibilities available for passive users to opt out of Analytics and DoubleClick cookies via third-party websites are also labour-intensive (especially for visits from mobile devices) and not (adequately) effective (if the cookies have already been placed and read before the user has had a chance to make a choice). If passive users decide to set their browser to refuse all cookies, they experience major disadvantages. Many websites (including websites without Google cookies) often function less well when all cookies are refused. In order to refuse the Google Analytic cookies, users must install a special plug-in, for each browser and each device that they use. There is no option for opting out of the use of the data on website visits for product development purposes.

The substantial usage share that the various Google services have in the Netherlands also plays a role in assessing the impact of the data processing operations on the data subjects' privacy. In addition to a usage share of more than 90% for Search, the Google Display network has more than two million websites, videos and apps worldwide; more than 20% of the nearly 8,000 most visited websites in the Netherlands contain DoubleClick advertisements and more than 65% contain Analytics code. In practice it is almost impossible for a Dutch Internet user not to interact with Google even without opening a Google account, be it via Search, YouTube or Maps, or passively through third-party websites by way of DoubleClick or Analytic cookies.

As alternative to the assessment that when using personal data obtained with the aid of tracking cookies Google can only claim unambiguous consent as a legal ground for the resultant or associated data processing, the Dutch DPA concludes that Google

cannot appeal to a legal ground under Article 8, opening words and (f) of the Wbp for the four examined forms of data processing involving the combining of data about and from various services, primarily because of the absence of necessity (proportionality and subsidiarity test) and additionally – in the alternative – because of the absence of safeguards such as transparency and effective opt-outs. Because of the nature of the data, the diversity of the services, and the lack of adequate and specific information and accessible and effective opt-outs, Google's legitimate interest does not outweigh the data subject's right to protection of his privacy. Because of this, Google does not have a legal ground as referred to in Article 8, opening words and (f) of the Wbp.

In its written view, Google writes that the Dutch DPA's assumption that Google must offer a general and central right to object is lacking sufficient basis in the law and has a disproportionate impact, in view of the negative consequences for Google and the limited user interests that the legislator sought to protect.[313]
The Dutch DPA's response to this is as follows. The sensitive nature of data such as payment information, location details and data on surfing behaviour across multiple websites, the extremely diverse nature of the services offered and the large scale of the data processing (usage shares in the Netherlands) make it necessary that Google take adequate measures to guarantee that the combining of data is strictly limited to what is necessary in the context of the legitimate purposes and that the data subject's right to protection of his privacy does not prevail. The specific and partial opt-out possibilities that Google offers are not adequately effective and user-friendly.

Because Google does not obtain unambiguous consent for the data processing operations investigated and has no other legal grounds pursuant to Article 8 of the Wbp, by combining data for the four examined actual purposes Google acts in breach of Article 8 of the Wbp.

5. Conclusion

GPP2012

Google's new privacy policy, which was introduced on 1 March 2012, states that Google can combine data from all its services with data from other Google services (including cookies which it sets and reads via third-party websites). This report investigates four purposes for which Google combines data: the personalisation of requested services, product development, display of personalisedpersonalised ads, and website analytics.

The Dutch DPA distinguishes between three types of users: authenticated users (signed in with a Google account), unauthenticated users (people using services such as Search without a Google account), and passive users (people who visit third party websites with Google cookies).

[313] Google's written view, paragraphs 71-75.

Applicable law and data controller

The *Wet bescherming persoonsgegevens* (Wbp) [Dutch Data Protection Act] governs the processing of personal data by Google Inc. Google Netherlands B.V. is the establishment of Google Inc. in the Netherlands in the context of whose activities the processing of personal data is carried out (Article 4(1) of the Wbp).

Personal data

Google collects and processes personal data as defined in in Article 1(a) of the Wbp from all three types of users. In many cases Google collects these data with the aid of tracking cookies. This is governed by the legal presumption contained in Article 11.7a of the *Telecommunicatiewet* (Tw) [Telecommunications Act] that this constitutes the processing of personal data.

Purposes

Because the examined purpose specifications described in GPP2012 and Google's new stated purpose of its data processing activities, i.e. 'the provision of the Google service', are ambiguous and insufficiently specific, Google does not collect the data for specific purposes and is therefore acting in breach of the provisions of Article 7 of the Wbp. Because Google has no legal ground for processing the data for the four examined purposes, the personal data collected by Google from all three types of users are not being collected for legitimate purposes (as being examined here), with the result that Google is acting in breach of the provisions of Article 7 of the Wbp in this respect as well.

Information

Because of the lack of information on its identity as data controller on the YouTube website, the fragmented and inconsistent method of providing information and the lack of specific information about the types of personal data and the purposes for which Google combines these data, Google is acting in breach of the provisions of Articles 33 and 34 of the Wbp. Google is acting in breach of the provisions of Article 33 of the Wbp insofar as it receives the personal data directly from the data subjects (from authenticated users when they create a Google account and from unauthenticated users when they use Search or carry out an action such as uploading a video to the YouTube servers). Google is acting in breach of the provisions of Article 34 of the Wbp insofar as it receives the personal data by a means other than directly from users or data subjects (e.g. data on the use of Google services and visits to third-party websites via DoubleClick and Analytic cookies).

Legal ground

Google has stated that it has a legal ground for processing the data under Article 8, (opening words) and (a), (b), or (f) of the Wbp.

Unambiguous consent

With regard to the legal ground for consent, Google often collects personal data with the aid of tracking cookies and thereby does not meet the consent requirement in Article 11.7a of the Tw and the obligation to provide users with clear and complete information in accordance with the Wbp. This applies to both its own websites and those of third parties. Google must also have a legal ground for the examined data

processing activities pursuant to Article 8 of the Wbp. In view of the similarities with Article 11.7a of the Tw, and in view of the intention of the European legislator to provide the same level of protection under both statutory standards and the overlap between the definitions of consent and unambiguous consent, it would seem logical to assume that there is a requirement for unambiguous consent for the personal data processing activities associated with the cookies (including the processing activities resulting from them).

However, there is no evidence of unambiguous consent as referred to in Article 8, opening words, and (a) of the Wbp, since Google does not offer data subjects any (prior) options to consent to or reject the examined data processing activities.

Insofar as Google claims that acceptance of its general terms of service and privacy policy amounts to consent, it is evident from the legislative history that unambiguous consent cannot be obtained through general terms of service. The legislative history also tells us that 'unambiguous' means that the data controller may not assume consent based on the failure to act or silence on the part of the data subject. However, Google assumes tacit consent and offers, at most, partial opportunities to opt out.

Finally, consent – unambiguous or otherwise – requires the information to be specific and the data subject to be informed. As shown above, Google does not adequately inform users about the fact that it combines personal data from different services, with or without the aid of cookies.

Necessary for the performance of the contract and legitimate interest
Because Google in many cases uses tracking cookies for the combining of personal data for the four examined purposes, unambiguous consent is as a rule required for the associated data processing activities. Therefore, claiming a legal ground under Article 8, opening words , (b) and (f) of the Wbp will not succeed for these reasons alone.

Google has not demonstrated and this investigation has not shown that the investigated data processing activities relating to the combining of data about and from multiple services are necessary (i.e. meet the requirements of proportionality and subsidiarity).

With regard to claiming a legal ground under Article 8, opening words, and (b) of the Wbp, there is no justification for the processing activities under investigation in its relationship with the specific individual data subjects (and any agreement entered into with them). Passive users will in most cases not even be aware that they have or will encounter Google cookies when using third-party websites. The terms of service therefore certainly do not give rise to a contractual relationship with passive users.

With regard to claiming a legal ground under Article 8, opening words, and (f) of the Wbp, Google has not argued convincingly that its legitimate interest in processing the data for the four purposes under investigation outweighs the data subject's right to the protection of their privacy. The combining of data by Google from and about multiple services and third-party websites for the purpose of displaying personalised

ads, personalisation of services, product development and analytics constitutes a major intrusion into the privacy of the users involved.

Some of these data are of a sensitive nature, such as payment information, location data and information on surfing behaviour across multiple websites. What is more, Google offers highly diverse services which serve entirely different purposes from the point of view of users (browsing, email, viewing videos, consulting maps).

Because of the nature of the data, the diversity of the services, the lack of adequate and specific information and the lack of effective opt-outs, Google's legitimate interest does not outweigh the data subject's right to protection of their personal data and privacy (this applies to all three types of users).

The considerable usage share the various Google services have in the Netherlands also plays a role in assessing the impact of the data processing activities on the data subjects' privacy. In practice it is almost impossible for a Dutch internet user not to interact with Google even without opening a Google account, be it via Search, YouTube or Maps, or passively through third-party websites by way of DoubleClick and/or Analytic cookies.

In addition, Google has failed to put adequate safeguards in place to ensure that the combining of data is strictly limited to what is necessary in the context of the legitimate purposes and that the data subject's right to protection of their privacy prevails.

Alternatively to the view that when using personal data obtained with the aid of tracking cookies Google can only claim unambiguous consent as a legal ground for the resultant or associated data processing activities, the Dutch DPA concludes that Google cannot claim a legal ground under Article 8, opening words, (b) and (f) of the Wbp for the four examined forms of data processing, primarily due to the absence of necessity and secondarily, when invoking Article 8(f) of the Wbp, due to the absence of safeguards such as transparency and effective opt-outs.

With regard to all three types of users, there is no legal ground as required under Article 8 of the Wbp for the combining of data for the four actual purposes that have been examined in this report. Google does not obtain unambiguous consent for the examined data processing activities and has no other legal grounds under Article 8 of the Wbp. For this reason, by combining data from and about multiple services for the four examined actual purposes Google is acting in breach of Article 8 of the Wbp.

Appendix I - Google's written view with response from the Dutch DPA