Google France SARL
38, avenue de l'Opéra
75002 Paris
France

Tél: +33 (0) 1 42 68 53 00
Fax: +33 (0) 1 53 01 08 15
www.google.fr

April 5, 2012

Isabelle Falque-Pierrotin
Presidente
CNIL
8, rue Vivienne
75002 Paris, FR

Re: Google

Dear Madame la Presidente,

Thank you for your letter and questionnaire of March 16, 2012, responding to our letter to you of February 28, 2012. We are happy to provide the additional information you request. Your questionnaire is wide ranging, covering a number of technical and legal areas in detail. Only some of the 69 questions you ask relate to our new Privacy Policy changes specifically, with many of the questions exploring broader privacy matters. While we are committed to providing the CNIL and all European data protection authorities with answers to the questions asked, we will, as agreed with your staff, need slightly longer than the time you have suggested to respond. As an interim step, we attach our responses to questions 1 to 24. The rest will follow as soon as complete.

In addition to our written responses, Google would, as noted in our letter of February 28, 2012, also welcome the chance to meet with the CNIL to explain and discuss Google's approach to providing information to users. This is an important issue for us. We have taken a great deal of time and care in designing our approach. In our very first letter to the CNIL on this topic, we emphasised that while we did not feel able to pause the implementation of our Privacy Policy, we would welcome the opportunity to discuss how and where Google provides information to our users. We have reached out many times to the CNIL asking for a meeting to discuss this, and we make that offer again now. We would also welcome attending a Working Party plenary to discuss the concerns of European data protection authorities more generally and to answer their questions.

Google's Approach to Providing Privacy Information

As context, it may be helpful to explain Google's approach to providing privacy information to users of Google services. Google believes that privacy policies should be both simple and comprehensive. The Working Party has recognised that it is not easy to write privacy policies

that achieve this important balance. We have worked hard to create a Privacy Policy that is user-friendly, readable and comprehensive, but that is only part of the picture.

Google provides additional privacy information to our users, in places where they expect to find it, at the times they want it. This use of such contextual in-product notices, in conjunction with our overarching Privacy Policy, work together to provide Google's users with meaningful privacy information and choice. We are always assessing where and how best to communicate privacy choice to users through product notice and design. We think that it is important to provide users with meaningful notice and choice within our products. We want to avoid an approach that sees notices become unwieldy and inaccessible to our users or that encourages companies to write notices as legal disclaimers.

We encourage the CNIL to examine the totality of the information Google provides its users, and how we deliver it, and not just focus on one piece of it, namely the Privacy Policy. As the Working Party is well aware, providing all detailed privacy information relating to all Google services in one Privacy Policy document would result in a tome with dozens of pages. Instead, we think we are doing a good job on providing a readable umbrella Privacy Policy together with detailed in-product privacy notices. In any case, we are also happy to consider and discuss any comments or views of the CNIL or the Working Party with respect to additional information they consider might be helpful to provide to our users in Europe.

We have provided at Appendix 2 a range of examples of Google's in-product privacy notices, to give the Working Party a better understanding of the breadth and scale of our privacy notice architecture. We would highlight the following examples which we believe are illustrative:

- In Google+, the initial default is to share with no one (the user has to choose which circles, individuals, or broader choices--public and extended circles--they want to share it with). Then their selection is sticky, so that next time they go to share something, those same people, circles, and original choices appear in the user interface.

- In Find my Face, which Google launched in December, the first time an individual is notified they are given basic information about how photos of them on Google+ are used to automatically suggest that other users tag them in photos uploaded to Google. This basic information has a link which allows the individual to "learn more". This is the classic short notice/long notice layered model about a specific type of data with a specific purpose.

- In Gmail, there is the "Why this ad?" link in ads that appear at the top and bottom of users' inbox and emails. When clicked, the user is given a brief explanation that the ad is based on emails in their inbox, and a second link that users are informed will take them to information to learn more, block specific advertisers or opt out of personalised ads.

Google's Approach to Sharing Information

Users are accustomed to their products working together, and expect this consistent experience across their Google Account. The use of a primary privacy policy that covers many products and enables the sharing of data between them is an industry standard approach adopted by

companies such as Microsoft, Facebook, Yahoo! and Apple.

Giving users easy access to their data across Google products allows them to do useful things such as immediately add an appointment to Calendar when a message in Gmail looks like it's about a meeting; read a Google Docs memo right in Gmail; use Google+'s sharing feature, Circles, to send driving directions to family and friends without leaving Google Maps; and use a Gmail address book to auto-complete contact's email addresses when inviting them to work on a Google Docs memo or sending them a Calendar invitation to a meeting.

Our updated Privacy Policy reflects our efforts to create one beautifully simple, intuitive user experience across Google. 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.

Most of our product-specific privacy policies allowed for sharing of information across products with a Google Account prior to this change. A few did not. Specifically, our policies meant that we couldn't combine data from YouTube and search history with other Google products and services to make them better. So if a user who likes to cook searches for recipes on Google, we are not able to recommend cooking videos when that user visits YouTube, even though he is signed in to the same Google Account when using both. We wanted to change that so we can create a simpler, more intuitive Google experience – to share more of each user's information with that user as they use various Google services.

It's also important to remember that even after the changes, users will still be able to use many of our products – such as Google Search and YouTube – without having to log into their Google Account or having to create one in the first place.

We will continue to develop new product features in line with our privacy principles by, among other things, being transparent about our practices and providing users with clear choices about how their data is used across our services. For example, users who log in can use the search history settings to edit or delete their search histories or turn off the product entirely. So a user who doesn't want search history used for other products can simply delete it or turn it off, consistent with our longstanding commitment to user control.

The updated Privacy Policy does not change users' existing privacy settings, nor does it result in any new or additional sharing of their personal information with third parties.

Pre-Briefing DPAs

Before we informed users of our plans to revise our Privacy Policy, we reached out to individual DPAs and asked whether we could visit them to offer a pre-briefing on the proposed Privacy Policy. In Europe alone, we provided pre-briefings to 18 DPAs. Of course, not all DPAs wanted a pre-briefing. This extensive outreach to regulators has, on the whole, been a constructive process. The feedback offered by the regulators we met was helpful. Significantly, none of the DPAs whom we pre-briefed asked us to "pause" our proposed launch of the Privacy Policy prior to Google communicating these changes to our users.

Communicating Changes to our Privacy Policy - Informing Users

We undertook the largest user notification campaign in our history. It was important to us that we did as much as we reasonably could to inform users about the changes and explain them clearly. Our notification to users included:

- an email to every email address associated with a Google account or service;
- a promotion on the Google.com and other country domains homepages;
- in-product notifications on properties often visited by unauthenticated users, such as Google Maps, Google News, iGoogle, mobile search and YouTube;
- a “New” icon next to the Privacy link on many Google pages; and
- an interstitial when users log into their Google Account both on computers and mobile devices. This interstitial could only be dismissed by the users clicking to “learn more” or “OK, got it”.

Working Party’s Request that we “Pause” the Launch of our Privacy Policy

After we had completed our DPA pre-briefings and our extensive, global notification campaign for users (which included sending hundreds of millions of emails to users), the Working Party asked us to "pause" the launch of our Privacy Policy. We realise that the decision not to pause has disappointed the Working Party. But after such an extensive notification it was difficult to see how such a pause was practically possible. At a practical level, “pausing” would have required us to launch yet another mammoth notification campaign, and would have proved confusing to our users.

Public Comments by EU DPAs

Following Google’s decision not to “pause” the launch of its Privacy Policy, some EU DPAs publicly criticised us, "raising strong doubts about the lawfulness" of our new Privacy Policy. Further, DPAs have made numerous comments to the media before they had addressed a single question to Google, or responded to our numerous requests for a meeting to discuss the issues.

We find it disappointing that some regulators publicly express doubts of lawfulness without having accorded us any chance to engage on the issues of concern.

Moreover, there are several important legal and procedural questions that emerge not just for this review but for any future co-ordinated efforts by the Working Party:

1) What is the legal basis for the Working Party to act as a regulatory body, or to mandate the CNIL to conduct a regulatory review on behalf of 26 other independent DPAs?
2) What law is being applied to this review?
3) Could the Working Party explain the process being followed and the ultimate aim of the review?

Commitment to collaborating with the Working Party

We hope that the answers provided with this letter, as well as the substantial additional

information we have provided on areas not covered by the questionnaire, demonstrate our willingness to engage on this issue with the Working Party. Google is committed to providing our users with comprehensive privacy information, and empowering them with privacy choices, not only in our Privacy Policy, but also in our in-product privacy notices. We are convinced that the overall package of our privacy notices respects completely the requirements of European data protection laws.

In the spirit of transparency, we plan to publish this response, together with our answers to the 69 questions you have asked and published.

Once again, we reiterate that we are happy to collaborate with members of the Working Party, and have made that clear from our pre-briefings and in our formal correspondence. In the spirit of fairness, we request the opportunity to be heard at a plenary session of the Working Party to answer questions and address the issues raised in your letters.

Respectfully submitted,

Peter Fleischer
Global Privacy Counsel

Appendix 1 - Responses to questions 1-24

2. The transition to the new privacy policy

QUESTION 1. Please indicate if Google implemented a process to answer questions from users since the announcement of the new privacy policy on January 24, 2012.

Yes, we provide a process to answer questions from users through our Privacy Policy, which states: "Your privacy matters to Google so whether you are new to Google or a long-time user, please do take the time to get to know our practices – and if you have any questions contact us".

The highlighted words "contact us" in the Privacy Policy link to a "Privacy Troubleshooter" which, among other things, specifically addresses the update to the Privacy Policy (see: "I have a question about the updated privacy policy"). By using the Troubleshooter, users can learn what the update to the Privacy Policy means to them, how they can delete their account, etc. If the user would like to ask additional questions, the Privacy Troubleshooter refers to a privacy contact form, which can be used for that purpose. Alternatively, as explained in the Privacy FAQs, users can write to:

> Privacy Matters
> c/o Google Inc.
> 1600 Amphitheatre Parkway
> Mountain View, California, 94043

USA

As set out above, we also note that we conducted the most extensive user notification effort in Google's history.

QUESTION 2. Please provide the approximate number of complaints/demands/questions addressed to Google following the announcement of the new privacy policy in January 2012.

It is not clear to us whether you refer to inquiries from media, regulators, or users or a combination of the above. We received roughly 1000 inquiries from the media. With regard to regulators, this is the only questionnaire we have received from any EU DPA, and we have received questions from a number of non-EU DPAs. Although Google manages user complaints in various ways, we do not record the specific information you are seeking. However, anecdotally, complaints from our users appear to have been minimal.

QUESTION 3.

A) Please provide the number of unique visitors that visited Google's dedicated privacy main site (http://www.google.com/intl/en/policies/ and localised versions).

We are unable to provide this particular metric, however, 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. Visiting a Privacy Policy home page is only one of these many mechanisms. Moreover, as noted above, Google undertook the largest user notification campaign in our history. It was important to us that we did as much as we reasonably could to inform users about the changes and explain them clearly.

B) Please compare it to the total unique visitors of Google's websites.

Please see above.

C) Please provide the same figure for the previous change in October 2010.

Please see above.

3. Services and collected data

QUESTION 4. Google's privacy policy uses various terms such as "information", "personal information" and "personally identifiable information". Please confirm that for the purpose of the new privacy policy, they should be understood by end users as all equivalent to "personal data" (as referred in the introductory definitions of this questionnaire).

For the purposes of the Privacy Policy the term "personally identifiable information" is used interchangeably with the term "personal information". The term "information" is used more broadly and covers the collection of information associated with anonymous identifiers.

As the Working Party is well-aware, the term "personal data" as defined in the Data Protection

Directive (95/46/EC) is in fact interpreted differently throughout the EU. Furthermore, in many non-EU jurisdictions definitions of “personal data” or “personal information” are used that are similar, but not necessarily identical, to the term as defined in the Data Protection Directive. In light of this, Google decided to define the term “personal information” in a manner that is simple to understand for users irrespective of where they are located, or to which particular data protection regime they are subject.

QUESTION 5.

A) Please provide the complete list of Google’s processings and services covered by the new privacy policy.

Google’s main consumer-facing products are listed at: www.google.com/intl/en/about/products/index.html.

The updated main Privacy Policy, in conjunction with the various in-product notices referred to in this letter, cover all relevant Google products, features and services with limited exceptions, as explained below. The Privacy Policy and notices collectively cover all associated processing activity which requires to be notified. You can find a sample of our in-product notices at Appendix 2.

Additionally, we’re maintaining three product-specific privacy notices, linked to from the main Privacy Policy: Google Wallet, Google Books and Chrome. These are explained in our Privacy Policy as follows:

> “**Specific product practices**
> The following notices explain specific privacy practices with respect to certain Google products and services that you may use:
> - Chrome and Chrome OS
> - Books
> - Wallet”

Google Wallet is a financial service and therefore regulated by industry-specific privacy laws. For Chrome and Books, we wanted to explain our privacy practices specific to those products in more detail without cluttering up the main Privacy Policy.

In addition, we are currently keeping the following standalone privacy policies or notices, some of which are carried over from recent acquisitions (which are identified with an asterisk after the name), and others which require their own separate privacy policies due to legal requirements or contractual commitments: AdMob*, BeatThatQuote, CleverSense*, Google Jobs, Google Health, InviteMedia*, Location Services in Firefox, reCAPTCHA, Teracent*, The Dealmap*, and Zagat*.

B) Please also indicate for each processing if it corresponds to a particular Google service (for instance, a processing related to security may cover several or all services).

Providing our consumer-facing services inherently involves a wide variety of processing activities from the collection until deletion of the data. As described in the Privacy Policy, 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”. As stated above, in addition we provide a range of contextual in-product notices for particular services (see Appendix 2 for examples).

QUESTION 6. For the following categories of data please detail the service(s) in which such data is processed and the purpose(s) of this processing:

As described in the Privacy Policy, 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”.

The updated Privacy Policy also 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 treat the user as a single user across all Google products to enhance user experience.

Under the headings below, we have highlighted the primary services for which such data elements are used:

A) “credit card data”,

Google users may choose to share their credit card information with Google in order to make purchases through Google Wallet or participate in loyalty programs through Google Offers.

We retain a separate privacy notice for Google Wallet that explains how we may use financial information associated with Google Wallet, including credit card data. We will not share users’ credit card information with retailers without obtaining users’ opt-in consent, except in the limited circumstances described in the Wallet privacy notice.

Through Google Wallet, users can purchase products offered on Google platforms, such as Google Play. Google Play is a one-stop shop for purchasing apps, songs, books, and movies. Google does not share the user’s full payment details with merchants who sell products on Google Play, and only shares users’ payment details as necessary to process the transaction.

B) “device-specific information”,

We process device-specific information in some cases when a user accesses a Google service from a particular device. For example, like most websites, our servers automatically record the page requests made when a user visits our sites. These “server logs” may also include device-specific information, such as the operating system version. As a further example, a user’s hardware model may be used to identify the appropriate format and interface to present to the relevant device, such as when web pages are configured to display differently on mobile device screens compared to full computer screens.

C) “telephony log information”,

Telephony log information will primarily be used for the Google Voice service. The purpose for processing telephony log information is to provide and improve the service, including by

troubleshooting in case of any issues.

D) "location information",

As stated in our Privacy Policy, Google may collect and process information about a user's location when using location-enabled services. The exact purpose for processing location information depends on the service and may also depend on user choices about how the location information is used.

Current examples of services that can be location-enabled are Google Maps, Google Latitude and location sharing in Google+. We are not collecting any new or additional information under the updated Privacy Policy. Nor are we changing the strong protections that we provide for location information. We collect location information tied to a Google Account on an opt-in basis, such as when a user has clearly chosen to have it collected for a personalised service such as Google Latitude or location sharing in Google+.

E) "unique device identifiers".

As a subset of device-specific information, we may process unique device identifiers when a user accesses a Google service from a particular device, or in some cases, via a particular network. For example, connections to services via WiFi will contain the MAC address, which is the unique ID of the router of the WiFi access point. We may collect a unique device identifier to provide services, such as sync functionality for a Google user's email and contacts, for Android devices.

QUESTION 7. The new privacy policy describes a list of "Information that we get from your use of our services" and includes in this description "Device information", "Log information", "Location information", "Unique application numbers", and "Cookies and anonymous identifiers". Please indicate if this list is comprehensive or if Google may collect additional data related to the user's use of its services.

The Privacy Policy and, where appropriate, supplemental in-product notices more fully described in this letter (see Appendix 2), provide the required notification of the information that Google collects in the context of the provision of its services. The categorisation noted is illustrative but not necessarily exhaustive. The key point is that we provide adequate notification in the contexts in which we think it is most useful for our users.

QUESTION 8. The new policy states: "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."

A) If a user does not have a Google Profile, please confirm that the user is not concerned by these sentences or detail how he may be affected.

That is correct.

B) Please confirm that all users can delete their Google Profile.

Indeed, users can delete their Google Profile. They can achieve this in two ways. First, users can always delete their Google account, which would cause their Profile to be deleted. Additionally, a user can downgrade from Google+ through their settings menu. They can choose to simply disable Google+ content or they can delete their entire Google Profile. The process to achieve this is explained on the Google + downgrade page: https://plus.google.com/downgrade and the "how to" page: How to downgrade from Google+.

C) Please indicate the list of services that are not available without a Google Profile.

There are several services that depend on a Google Profile: Google+, Buzz (which is no longer in use, but users may currently still choose to have old Buzz activity associated with their Profile) and Profile itself.

Other services that require a Profile are +1s (in search, ads, etc.), Google+ social integrations across all products (for example, sharing other than by email in Google Reader requires a Profile, but reading in Reader does not), Google Photos (as distinct from Picasaweb, which can be used without a Profile).

QUESTION 9. The new privacy policy states: "We require opt-in consent for the sharing of any sensitive personal information."

A) Please describe when, how and in which services sensitive data may be collected by Google.

Google does not require users to provide any sensitive data. Google users themselves can, however, decide to share information about their health, for example, on Google+. Users could also store sensitive data on services such as Gmail, Google Docs and Google Calendar.

Google users may also choose to enter, for example, health related search terms, in which case Google may display relevant search results and ads based specifically on the search terms. As explained in the Privacy Policy, when showing the user tailored ads, Google will not base the serving of that ad with any sensitive categories set out in the Data Protection Directive.

Please note that Google Health has been discontinued as of January 2, 2012, as explained here: http://www.google.com/intl/en_us/health/about/index.html.

B) Please provide the purposes of such collection.

Please see above.

C) Please confirm that Google defines « sensitive data » as referred in the introductory definitions of this questionnaire.

Yes, we can confirm that we apply the definition of sensitive data as set out in the Data Protection Directive appropriately in the context of providing our services.

QUESTION 10. Please describe how and in which cases "opt-in consent" is (or will be) collected

for the sharing of sensitive data.

As per above, Google does not require users to provide any sensitive personal data, but users may choose to do so. The primary choice to share sensitive personal data rests with users. For example, they can share a Google Doc or Google+ post containing such data.

The Privacy Policy additionally makes clear that if Google intended to share any sensitive personal data, it would first obtain user consent, except for the legal reasons set out in our Privacy Policy.

QUESTION 11. Google does not mention face recognition in its new privacy policy. Does this mean that Google does not use facial recognition processings or that a specific policy will apply for such processing. In this case, will Google ask users for prior explicit consent before applying face recognition to pictures or other material uploaded by users (for example a picture used for a Google account, or pictures uploaded to Google+ representing the user or third parties)?

Google uses facial recognition technology in its Google+-service, which is covered by the Privacy Policy.

Indeed, Google + Find my Face asks users for prior consent before creating a facial recognition model for the user that might be used to suggest photo tags to other users. If the user gives his/her consent, Google+ can prompt people who know the user to tag the user's face when they upload photos. The user has control over which tags he/she wants to accept or reject and can always turn the feature off in the Google+ settings. This feature is explained in plain and simple language when new Google+ users register for the Google+ service, see for example below:

> " **Help people tag you in photos**
> By turning on Find My Face, Google+ can prompt people you know to tag your face when it appears in photos.
> Of course, you have control over which tags you accept or reject, and you can turn this feature on or off in Google+ settings. Learn more
>
> Turn on Find My Face
> No Thanks

QUESTION 12. The use of many Google services results in the creation of a PREF cookie, such as in the following example: PREF=ID=3a391cb61c62dbb1:TM=1331203931:LM=1331203931:S=ZRtXLvbm7vQc3jbR; expires=Sat, 08 Mar 2014 10:52:12 GMT; path=/; domain=.google.com

A) Please confirm that the use of most online Google services (and especially services in the google.com domain) will result in the storage and access to a cookie called "PREF" in the user's terminal equipment for each interaction with the service (typically any http request) and that this cookie is not modified when logging in or out to one or several Google accounts.

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. When logging into Google, Google may add “GM=1” or “IG=1” to the PREF cookie if you are a Gmail or iGoogle user, respectively. This helps us gather aggregate information about the use of Google services by Gmail and iGoogle users, but it does not link the PREF cookie to a specific Google account. PREF cookies are not modified when users log out of their Google accounts.

B) Please indicate when, how and for which purposes information collected with this cookie is used.

Browsers will automatically send PREF on any request to google.com or its sub-domains. However, Google does not associate the PREF identifier with the user’s Google account. The PREF cookie may store user preferences and other information, in particular a user’s preferred language (e.g., French), how many search results users wish to have shown per page (e.g., 10 or 20), and whether or not they wish to have SafeSearch filter turned on.

C) Please detail the role of the “ID” component in this cookie.

This ID is standard industry-wide cookie architecture. The ID is the unique cookie ID assigned to a particular computer the first time it visited Google.

4. Purposes

QUESTION 13.

A) Please indicate which categories of personal data are used to “improve the services and develop new services”.

Google may use any information we collect from our users to improve our services and develop new services, which includes the categories listed under “Information we collect” as specified in the Privacy Policy.

B) Please indicate if Google uses sampling techniques and anonymisation/pseudonymisation processes for these purposes. If so, please provide the methods Google is using.

Where appropriate, Google uses the best techniques available to ensure the privacy of our users is protected when personal data is used in this context, including the techniques listed here. Some of the particular techniques we use are:

- Reducing the granularity of the data (e.g., age ranges rather than exact ages);
- Adding noise to the data (e.g., not using exact counts, but rather "fuzzing" the counts);
- Enforcing thresholds (e.g., a minimum number of users must have the attributes/have taken the actions, before we can use the data as inputs); and
- Requiring public evidence of personal associations.

QUESTION 14. Please provide examples of information Google collects and uses for the purposes of “protecting Google and its users”.

Google may use information that it receives in the context of the provision of its services for the purpose of protecting Google and its users.

A good example is the two-step authentication that Google introduced to add an extra layer of security to users' Google Account. In addition to the user's username and password, the user enters a code that Google will send to the user via text or voice message upon signing in, as explained in further detail here: http://support.google.com/accounts/bin/answer.py?hl=en&answer=180744.

Another example is the Google Chrome browser which includes features to help protect the user from malicious websites as the user browses the web. Chrome will, for example, show the user a warning message before the user visits a site that is suspected of containing malware or phishing, as explained in further detail here: http://www.google.com/chrome/intl/en/more/security.html.

For more information on how Google protects users and how Google educates its users on how to stay safe online, please refer to http://www.google.com/goodtoknow/online-safety.

QUESTION 15. Google indicates that it will also use "information to offer the user tailored content – like giving the user more relevant search results and ads". Besides search results and ads, please be more specific about the different types of tailored content Google provides to the user.

Two examples would be the use of a Gmail address book to auto-complete a contact's email address when you invite him/her to work on a Google Docs memo or send him/her a Calendar invitation to a meeting and personalisation of home page content such as local language choice or the iGoogle product.

QUESTION 16. Please provide the list of Google services that collect information from users for the purpose of providing "more relevant search results" to the user.

As explained in the Privacy Policy, all of our services may collect information from users for the purposes of providing more relevant search results.

Depending on whether or not the user is signed in to a Google Account when the user searches, the information Google uses for customising the user experience will be different:

Signed-in personalisation: When the user is signed in, Google personalises the user's search experience based on the user's Web History. The user can turn off Web History and remove it from the user's Google Account. The user can also view and remove individual items, as well as pause his/her Web History. The user can also turn off personal results to prevent personalisation based on the user's Web History. Turning off personal results will also disable several other personalisation features, such as the ability to search across content shared by the user's friends and connections. The user may see annotations beneath results that have been personalised by the user's Web History. The annotations may indicate how many times a user visited the page, when she last visited the page, or a previous search term related to the page.

Signed-out personalisation: When a user is not signed in, Google personalises that user's search experience based on past search information linked to the user's browser, using a cookie. Google stores up to 180 days of signed-out search activity linked to the user's browser's cookie, including queries and results the user clicks. Because many people might search from a single computer, the browser cookie may be associated with more than one person's search activity. For this reason, we don't provide a method for viewing this signed-out search activity. If the user does not want to see results personalised based on this search history while the user is signed out, the user can turn off search history personalisation.

We provide the following illustration of the information we use in each case:

	Signed-in search history personalisation	**Signed-out** search history personalisation
Where the data we use to customise is stored	In Web History, linked to your Google Account	On Google's servers, linked to an anonymous browser cookie
How far back we use search history	Indefinitely or until you remove it	Up to 180 days
Which searches are used to customise	Only signed-in search activity, and only if you have Web History enabled	Only signed-out search activity
How to turn off	Turn off search history personalisation ("Signed in searches" section)	Turn off search history personalisation ("Signed out searches" section)

QUESTION 17. Please provide the list of Google services that collect information from users for the purpose of providing "more relevant ads" to the user.

As explained in the Privacy Policy, all of our services may collect information from the users for the purposes of providing more relevant and useful ads. By way of illustrative example, the manner in which we provide more relevant ads in Search and Gmail is explained through a short video and additional information here: http://www.youtube.com/watch?v=PN0I_YIDF1A.

We also offer transparency & control to our users through the Ads Preferences Manager. As explained in the Advertising privacy FAQs, the Ads Preferences Manager is a Google site where the user can manage settings associated with the ads that the user sees.

QUESTION 18. Please detail how Google plans to collect user consent "before using information for a purpose other than those that are set out in this Privacy Policy".

The appropriate manner and form in which to request user consent or provide additional user notice necessarily depends on the specific context of the product or service. It is not feasible to predict now which manner or form would be appropriate for obtaining such user consent in the future should it be required.

5. Data retention

QUESTION 19.

A) Please explain why Google "may not remove information from […] backup systems", when the user asks for its deletion.

We delete users' personal information at their request in line with our back-up and retention policies. Google's back-up and retention policies are set to take into account users' interest in security and business continuity.

We operate reliable, world-class backup systems to protect our users against accidental or malicious deletion of their information. For example, by operating a backup system, we are able to help users recover data that may have been lost after their accounts were hacked. Our users expect and require this type of protection against data failures. Information kept on backup tapes is used only to restore lost data and is encrypted. It is not used for any other purpose including ad targeting or personalisation. Access is restricted to those teams that operate the system. In accordance with our back-up management schedule, we routinely delete encryption keys and reuse and destroy backup media as it degrades or fails. Removing data from our backup tapes is routinely achieved through disposal of the encryption keys, rendering the data inaccessible.

B) Please clarify if this means that data will actually be deleted from all backups after an additional period of time or not.

Google has documented policies and processes covering deletion of user data from back-up tapes.

C) Please provide an upper bound on the additional retention period needed to delete data from all backups.

The period primarily depends on the particular service or back-up system in question. This will necessarily vary from case to case.

QUESTION 20. Google's privacy FAQ indicates that Google anonymises IP addresses after 9 months and cookies after 18 months for its search engine service. For other services, please provide the maximum retention periods that are applicable to data regarding "non-authenticated users" and "passive users", including IP addresses, cookies and any other types of data. Please distinguish according to the different types of services.

Indeed, we anonymise IP addresses after 9 months and cookies in our search engine logs after 18 months.

For some services, we also use anonymous identifiers, which are periodically deleted based on inactivity. Users can reset or disable anonymous identifiers at any time using the Ads Preference manager for mobile applications. Instructions can be found here: http://www.google.com/policies/privacy/ads/#toc-apps.

For some services, we apply significantly shorter retention policies, consistent with the purposes for which the information is retained. For example, information about the partial queries users input into Google Search while they are typing into our Google Instant service is generally discarded after two weeks.

QUESTION 21. Please provide the maximum additional retention period for data deleted by authenticated users, following content withdrawal, service un-subscription and full account deletion.

We delete users' personal information at their request in line with our back-up and retention practices and policies. Google's back-up and retention policies and practices are set to take into account the user's interest in security and business continuity. Such policies would, for example, enable us to restore a maliciously deleted user account.

6. Rights & consent

QUESTION 22.

A) What does the sentence "We will not reduce your rights under this Privacy Policy without your explicit consent" mean? Please provide examples of reduction of rights that would require explicit consent according to Google's privacy policy.

As described in the Privacy Policy, and as is common practice in the Internet and other industries, Google may make changes to the Privacy Policy from time to time.

In making this change to the Privacy Policy, Google has not reduced any of the users' rights. Our main Google Privacy Policy has made it clear since 2005 that data collected by Google can be used to improve our products and services generally. The updated policy removes a few ambiguities and restrictions in how we can use data in a user's account to improve his/her experience across our products. Also, the Privacy Policy does not provide for any new external sharing.

B) In this respect, Google removed the sentence "we may give you the opportunity to opt out of combining such information", which appeared in the previous version of the privacy policy. Do you consider that the fact Google no longer gives the opportunity to opt-out of combining such information constitutes a reduction of the user's rights?

No, we believe that the relevant issue is whether users have choices and control about how their data is collected and used.

We would also emphasise that we have not changed any of our users privacy settings and that there is no new external sharing of information as a result of this new Privacy Policy.

We are not changing our commitment to not sell users' personal data, or limiting the tools available to users to exercise control over their data. For example, users can edit and delete their signed-in search history, control the way Google tailors ads to their interests using our Ad Preferences Manager, use Incognito mode on Chrome, switch Gmail chat to "off the record,"

or further control their information using any of the other privacy tools we offer. The Google Dashboard allows signed-in users to see a snapshot of the information associated with their Google Accounts and to manage that information using various privacy controls.

Our users will continue to have the ability to take their information elsewhere quickly and simply through our data liberation tools.

QUESTION 23. With regards to the previous question, how does Google plan to obtain "explicit" consent from users and in what circumstances? Please distinguish between users with a Google account and users not signed in or who do not have a Google account.

The appropriate manner and form in which to request user consent or provide additional user notice necessarily depends on the specific context of the product or service. It is not feasible to predict now which manner or form would be appropriate for obtaining such user consent in the future should it be required.

QUESTION 24. Does Google consider that the users who had a Google account before 1 March 2012 and who continue to use Google's services after March 1st thereby express consent to the new privacy policy?

If people continue to use Google services after March 1, they'll be doing so under the updated Privacy Policy. In addition, as noted throughout this response letter, we also provide contextual in-product notices and opt-in consents as the context requires.

As discussed above, the use of a primary privacy policy that covers many products and enables the sharing of data between them is an industry standard approach adopted by companies such as Microsoft, Facebook, Yahoo!, and Apple.

Appendix 2 - Examples of contextual notices in Google products

Enclosed separately.