APPENDIX
GOOGLE PRIVACY POLICY: MAIN FINDINGS AND RECOMMENDATIONS

OUTLINE

I. MAIN FINDINGS

1) LEGAL FRAMEWORK

Google's services[1] are available to natural persons in the European Union and the criteria of the European Directive to define applicable law are met. The European Data Protection law therefore applies to Google's personal data processing operations.

Google implements several personal data processing operations in the course of the provision of its services: a specific processing operation can be associated with each service and Google implements other processing operations for crosscutting purposes such as security, research, etc.

The Working Party identified three types of data subjects that use Google's services:

- Authenticated users (Gmail, Google Play, Docs, Google+, etc.)
- Non-authenticated users (Search, Maps, Youtube, etc.)
- Passive users (DoubleClick, Analytics, '+1' buttons)[2]

2) INFORMATION

Google's Privacy Policy fails to respect the obligation of information, laid down in section IV of the Data protection directive.

First, Google gives incomplete or approximate information about the purposes and the categories of data collected. The Privacy Policy is a mix of particularly wide statements and of examples that mitigate these statements and mislead users on the exact extent of Google's actual practices. Additional information is available in in-product privacy notices, the Help Center or blogs but the information available in these documents is inconsistent between the different sources or spoken languages, can be changed at any moment and is sometimes difficult to understand. The main Privacy Policy is the only traceable document (i.e. for which previous versions are still available). The Working Party notes in particular that the 60+ previous privacy policies that have been merged in the main Privacy Policy are not available anymore and that Google failed to provide the list of these 60+ privacy policies.

Regarding information on purposes, the purposes in the Privacy Policy are not detailed enough and do not respect the principle of purpose limitation. Either the purposes in the Policy are the *actual* purposes of Google's processings, in which case Google does not comply with Article 6(b)

[1] Google's services are provided in 22 of the 23 official languages of the European Union (all except Maltese – regional and other national official languages may also be available) and Google's services are available in 25 of the 27 main top-level domains of the Member States (all except .mt and .cy – google.eu is not available either). Besides the availability of Google's online services, devices running Google's software (mainly Android phones) are commercialized in most if not all Member States. Google also owns national companies established in several European countries (e.g. in the UK, Ireland and France), which are to some extent involved in commercial purposes, research and development, and public relations. Google's headquarters in Europe are located in Dublin, Ireland. Google uses servers located in the European Union to provide its services, including two major datacenters located in Belgium and Finland. Google also uses cookies and other means, stored on users' devices, to provide its services.

[2] Passive users, as defined in the questionnaire sent on March 16 are users who does not directly request a Google service but from whom data is still collected, typically through third party ad platforms, analytics or +1 buttons.

of the Directive (because purposes are not "specified and explicit"), or personal data are processed for more specific purposes that Google did not describe in the Privacy Policy and in its answers to the questionnaires: in this case, Google failed to comply with the obligation of information defined in Articles 10 and 11 of the Data Protection Directive.

Regarding information on the categories of data that are processed by the services, the categories described in the privacy policy are too broad and do not provide appropriate information to the data subject when he uses a particular service.

The actual use of data by Google in each service may not be excessive but in this case, information is insufficient with respect to the requirements laid down in Articles 10 and 11 of the Directive. Google also failed to provide elements that would guarantee the respect of the principle of data minimization. In particular, Google has not indicated what data is combined between which services.

Concerning passive users, users are generally not informed that Google is processing personal data, such as IP addresses and cookies. Information depends on the website's policy and may often not detail Google's processing.

3) COMBINATION OF DATA ACROSS SERVICES

Google uses many tools to combine data:

- The Google Account associated with each authenticated user
- The PREF cookie associated with each interaction with a website of the google.com domain (including '+1' buttons on third-party websites)
- The DoubleClick cookie associated with interactions on third-party websites that display DoubleClick advertisements
- The Google Analytics cookie used by third-party websites
- Mobile identifiers used to replace cookies on some mobile applications

The combination of data implemented by Google is very broad as it will include all the activity of data subjects on Google's sites[3] and activity on third-party websites ('+1' buttons, DoubleClick). Google also stores data during long periods of time: 18 months of browsing history for the PREF cookie, 2 years for the advertising cookie. Furthermore, the risks associated with the combination of data across services are high for the data subjects: data breach, rogue personnel, legal requests, etc.

The Working Party identified 8 different purposes for the combination of data across Google's services:

- The provision of **services where the user requests the combination of data (case #1)** (e.g. Contacts & Gmail)
- The provision of services requested by the user but where the combination of data applies **without the user's direct knowledge (case #2)** (e.g. search results personalization)
- **Security purposes (case #3)**

[3] Google has a European market share of around 90% for search and around 50% for smartphone OS

- **Product development and marketing innovation purposes (case #4)**
- The provision of the **Google Account (case #5)**
- **Advertising purposes (case #6)**
- **Analytics purposes(case #7)**
- **Academic research purposes (case #8)**

However, the tools used by Google such as the Google Account or the PREF cookie have use policies that are independent of the purposes, e.g. anonymisation of server logs after 18 months. Google does not differentiate the different purposes for the combination of data and does not clearly endorse the principle of purpose limitation.

Additionally, the Working Party examined the lawfulness of the combination of data in regards of the legal grounds set out in Article 7 of the Directive, namely "consent", "performance of a contract" and "legitimate interests".

For four of the eight purposes above, the Working Party has established the absence of a legal ground **for the combination of data across services**[4]. This is the case for the provision of services where the combination of data applies without the user's direct knowledge (case #2), marketing innovation and product development (#4), advertising purposes (#6) and analytics purposes (#7).

For these purposes, there is **no valid consent** from the user, in particular because the user is not aware of the exact extent of the combination of data. **Google's interests** to implement the extensive combination of data detailed above **are overridden by the interests for fundamental rights and freedoms of the data subject** and therefore, the legal ground of the legitimate interests may not apply, unless Google clearly limits the scope and duration of the combination of data and provides simple and effective rights to the data subjects. Finally, Google did not provide significant examples of combination of data realized for the performance of a contract that would justify such a large collection and combination of data.

Google may not claim to use any data from any service for these purposes without a valid legal basis. In order to remedy to this situation, **Google should seek consent from the data subjects for the combination of data for these purposes and provide additional controls to users regarding these combinations.**

The new Privacy Policy also applies to end-users of the Google Apps (Free) offer. In this case, consent may not be valid because the data subject is likely to be an employee of the customer of Google that decides to use this offer.

More generally and for all purposes, **combination of data must respect the principles of proportionality, purpose limitation, data minimization and right to object**. **Google does not publicly endorse these principles** and failed to provide clear and definite answers on these matters: there is no guarantee that only the data necessary to the purpose is combined, information is insufficient (cf. section "Information") and the current opt-out mechanisms are too complex and ineffective. For instance, a mobile authenticated Google+ user who does not want personalized ads must perform six different opt-outs. Moreover, some of the mechanisms do not prevent the collection of data, but only the display of personalized content. Finally, there

[4] The investigation does not asses the legal ground of Google's processing operations besides the combination of data.

are no opt-outs for the purposes of research or marketing innovation and product development except by not using the service.

For **passive users,** Google does not respect Article 5(3) of the ePrivacy Directive regarding cookies triggered by DoubleClick, '+1' buttons or Google Analytics services on third-party websites. Informed consent is necessary before these cookies are used for the purpose of data combination across services.

Regarding **Google Analytics** and the combination of data for analytics purposes, specific safeguards have been implemented for German users: data combination across services is excluded, a specific contract is signed between Google and the website, and customers can automatically anonymise the IP address shared with Google. Such conditions can provide adequate protection of personal data and should be extended to all European Member States.

4) RETENTION PERIOD

Despite the numerous and detailed questions of the Working Party, Google has been unable to provide a maximum or typical retention period for the personal data it processes. This absence of response questions the effectiveness of the opt-out mechanisms and deletion actions requested by the users.

The Working Party encourages Google to endorse the principle of retention period strictly limited according to the purposes.

II. RECOMMENDATIONS

Considering the conclusions of the investigation, Google should implement the following recommendations in order to comply with the Data protection legislation.

1) INFORMATION

To remedy the insufficient information about Google's processings, **Google must complete information about its processing operations by detailing for each processing the exact purposes and collected data (including data from other services).**

Information must describe the purposes and the categories of data processed in a clear and accurate manner. The processing operation itself must be conducted with due respect to the rules of proportionality and data minimisation, which must be reflected in the information that is delivered.

Moreover, notices about each processing must not be modified unless the user has given his consent, having been provided with clear and comprehensive information inter alia about the changes to be implemented; furthermore, notices should be traceable.

Practically, the Working Party recommends to **define an architecture of privacy notices** that would offer a simple and comprehensive information about the processing operations. Users

should have a clear visibility on this architecture and be able to navigate in ways that meet their expectations.

The architecture could adopt **the following three levels**:

First, **in-product privacy notices and interstitial notices** could be developed to increase user's awareness of the processing when they use the services and especially when they launch a new service for the first time. Tools such as the toggle button for "Search Plus Your World" or the "butter-buttons" used to inform about the change of Privacy Policy are also good examples of straightforward and timely information. Google should develop internal processes to systematically verify the level of basic user information regarding personal data protection for each of its existing and future services.

Second, the **current privacy policy** should be presented as a general guideline about Google's processing operations and references should be made to more detailed information about the different processings ("product-specific privacy notices"). Moreover, the Working Party recommends separating clearly the statements of the policy from illustrative examples, as these examples tend to mislead the users about the exact scope of the statements. Examples should also ideally cover different use cases. The Privacy Policy should include all types of categories of data, including biometric data, as face recognition is not mentioned in the current policy.

Third, **product-specific privacy notices** should be made available. Such notices should detail for each processing and service: the data that is processed, the purposes of the processing, the recipients and how users can access their data. General purposes such as research and security could be presented separately with detailed guarantees about these purposes. Previous versions of the privacy policy and of the product-specific privacy notices should remain available to users.

More generally, Google should develop **interactive presentations** that allow users to explore the content of the privacy notices without having to read long and linear documents.

Finally, Google should provide additional and precise information about the following data that may have significant impact on the privacy of users:

- Location
- Credit card data
- Unique device identifiers
- Telephony

Users must have simple and clear explanations on when, why and how such data are collected and how they can oppose to the collection, the storage or the combination of these data.

i. PARTICULAR CASE OF MOBILE USERS

Mobile users face the additional challenge to use Google's services on small screens, with limited interactions. Many of the features requested above may not appear or may not be delivered on mobile screens, especially in-product privacy notices or interactive presentations.

Google must provide adapted information for these users, possibly with specific tools that may include dedicated applications or privacy controls on Android.

ii. PARTICULAR CASE OF PASSIVE USERS

Regarding passive users, information is mainly delivered by third-party websites on which Google's services are implemented. Google must therefore make sure users are correctly informed about the processing operations that concern them.

2) COMBINATION OF DATA

Regarding the combination of data, Google lacks a legal basis for certain purposes. Furthermore, information about the combination of data is particularly weak and the recommendations of the previous section apply: Google must first reinforce information to clarify the data that is combined across services and the purposes for which data is combined.

i. FOR PURPOSES THAT HAVE A LEGAL BASIS FOR THE COMBINATION OF DATA (CASES #1, #3, #5, #8)

When using data from other services, Google must adopt a **Privacy by Design approach:** limited sets of personal data should be used, and anonymisation should be implemented, when possible (principle of data minimisation).

Simple opt-outs must be made available for the purposes where the right to object applies, i.e. provision of services requested by the user (case #1), research (#8) and Google Profile (#5). In general, opt-out for security purposes requires a cautious approach to avoid abuses.

Retention periods must be appropriate in regards to the purpose.

ii. FOR PURPOSES THAT DO NOT HAVE A LEGAL BASIS FOR THE COMBINATION OF DATA (CASES #2, #4, #6, #7)

Google must seek unambiguous consent from the data subjects for these purposes and limit clearly the scope of the combination of data in proportion with the purposes pursued.

In this context, the inclusion of a new service into the combination of data or a new purpose requires explicit consent (e.g. Google Now), that can be easily collected the first time a user wishes to use the new service.

The Working Party also advises Google to develop new tools to allow users to control which services may combine data. These controls can include:

- Specific settings in the Google Dashboard for authenticated users
- Explicit consent and improved control over cookies (and the data collected) for non-authenticated and passive users

iii. PRACTICAL RECOMMENDATIONS

The following practical recommendations could therefore be implemented by Google to ensure legal compliance of the combination of data:

1. Google should **simplify the opt-out mechanisms** and foresee new tools to implement the right to object to the combination of data for some of the purposes detailed above. In this regard, user should have a clear understanding of the purposes for which data is combined.

2. Google should **differentiate the purposes of the combination of data** with appropriate tools: the use of the PREF cookie ID for several purposes should be abandoned and cookies (or other tools) could be created for each purpose (security, advertising, service improvements) with retention policies and access rights related to the purpose.

3. Google should **collect explicit consent for the combination of data** for the purposes of service improvements without the user's direct knowledge, product development and marketing innovation, advertising and analytics.

4. Google should make the **opt-out mechanisms available in one place** for authenticated and non-authenticated users.

5. Google should offer the option for authenticated users to **control in which service they are logged in** when these services are available without authentication (e.g. Search, Maps or Youtube), typically with a setting on their account.

6. Google should limit the collection and combination of data from passive users, except for security purposes.

7. Google must **enforce Article 5(3)** of the ePrivacy Directive for passive users, with regards to the guidance provided in the WP29 Opinion on Cookie consent exemption.

8. For analytics purposes, Google should also **extend to all European users the process designed in Germany** (enhanced information of the data subjects by the website, limited use of the data to the purpose of analytics and IP anonymisation).

iv. PARTICULAR CASE OF GOOGLE APPS (FREE EDITION) USERS

For Google Apps end-users, the use of a Google Account is decided by the Google Apps customer (typically the company that employs the end-users): consent may therefore not be valid. Google should apply limitations to the combination of data across services and this combination should be restricted to the services included in the Google Apps offer.

3) RETENTION PERIOD

Google should define more clearly the retention period of personal data, especially for the following actions: deletion of a particular content, unsubscription of a specific service, deletion of the account.

III. OTHERS

1) NAME POLICY

Google must inform new users more clearly that they can sign-up to a Google account without providing their real name.

2) FACIAL RECOGNITION

Google must complete the Privacy Policy by mentioning that biometric data may be processed and clarify the conditions of collection and storage of the face template.

3) INTERNATIONAL TRANSFERS AND SAFE HARBOR

Google's compliance with the European rules applicable to international transfers and to the U.S.-E.U. Safe Harbor Agreement has not been investigated in this analysis.