00737/EN
WP 148

Opinion on data protection issues related to search engines

Adopted on 4 April 2008

Table of contents

EXECUTIVE SUMMARY

Search engines have become a part of the daily life of individuals using the Internet and information retrieval technologies. The Article 29 Working Party recognises the usefulness of search engines and acknowledges their importance.

In this Opinion the Working Party identifies a clear set of responsibilities under the Data Protection Directive (95/46/EC) for search engine providers as controllers of user data. As providers of content data (i.e. the index of search results), European data protection law also applies to search engines in specific situations, for example if they offer a caching service or specialise in building profiles of individuals. The primary objective throughout the Opinion is to strike a balance between the legitimate business needs of the search engine providers and the protection of the personal data of internet users.

This Opinion addresses the definition of search engines, the kinds of data processed in the provision of search services, the legal framework, purposes/grounds for legitimate processing, the obligation to inform data subjects, and the rights of data subjects.

A key conclusion of this Opinion is that the Data Protection Directive generally applies to the processing of personal data by search engines, even when their headquarters are outside the EEA, and that the onus is on search engines in this position to clarify their role in the EEA and the scope of their responsibilities under the Directive. The Data Retention Directive (2006/24/EC) is clearly highlighted as not applicable to search engine providers.

This Opinion concludes that personal data must only be processed for legitimate purposes. Search engine providers must delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for and be capable of justifying retention and the longevity of cookies deployed at all times. The consent of the user must be sought for all planned cross-relation of user data and for user profile enrichment exercises. Website editor opt-outs must be respected by search engines and requests from users to update/refresh caches must be complied with immediately. The Working Party recalls the obligation of search engines to clearly inform the users upfront of all intended uses of their data and to respect their right to readily access, inspect or correct their personal data in accordance with Article 12 of the Data Protection Directive (95/46/EC).

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive, and Article 15 paragraph 3 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002

having regard to Article 255 of the EC Treaty and to Regulation (EC) no 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents

having regard to its Rules of Procedure

HAS ADOPTED THE PRESENT DOCUMENT:

1. INTRODUCTION

Search engine providers on the World Wide Web fulfil a crucial role in the information society as intermediaries. The Working Party recognises the necessity and utility of search engines and acknowledges their contribution to the development of the information society.

For the independent data protection authorities in the EEA, the increasing importance of search engines from the perspective of data protection is reflected in the increasing number of complaints received from individuals (data subjects) about potential breaches of their right to a private life. A marked rise in requests has also been noted from both data controllers and the press about the implications of web search services for the protection of personal data.

The complaints from data subjects and the requests of data controllers and the press reflect the two different roles played by search engine providers with regard to personal data.

First, in their role as service providers to the users, search engines collect and process vast amounts of user data, including data gathered by technical means, such as cookies. Data collected can range from the IP address of individual users to extensive histories of past searching behaviour or data provided by users themselves when signing up to use personalised services. The collection of user data gives rise to many questions. After the AOL case a large audience was made aware of the sensitivity of personal information contained in search logs[2]. It is the opinion of the Working Party that search engines in

---

1 Official Journal no. L281 of 23/11/1995, p. 31, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 In the summer of 2006, the service provider published a sample of queries and results of some 650.000 users during a 3 months period. Even though AOL had replaced the names of the users by a number, journalists found out these results could often be traced to individual users, not only because of so-called 'vanity searches' (people searching for information about themselves) but also by combining several queries by a single user .

their role as collectors of user data have so far insufficiently explained the nature and purpose of their operations to the users of their services.

Second, in their role as content providers, search engines help to make publications on the internet easily accessible to a worldwide audience. Some search engines republish data in a so-called 'cache'. By retrieving and grouping widespread information of various types about a single person, search engines can create a new picture, with a much higher risk to the data subject than if each item of data posted on the internet remained separate. The representation and aggregation capabilities of search engines can significantly affect individuals, both in their personal lives and within society, especially if the personal data in the search results are incorrect, incomplete or excessive.

The International Working Group on Data Protection in Telecommunications[3] adopted a Common Position on Privacy protection and search engines on 15 April 1998, revised on 6-7 April 2006[4]. The Working Group expressed herein concern about the potential for search engines to allow profiles of natural persons to be created. This common position outlined how some search engine activities could cause a threat to the privacy of individuals, and that any kind of personal information posted on a website could be used by a third party for profiling.

In addition, the 28th International Data Protection and Privacy Commissioners' Conference adopted the Resolution on Privacy Protection and Search Engines[5], London, 2 – 3 November, 2006. The Resolution calls upon providers of search engines to respect privacy rules as laid down in national legislation in many countries, as well as in international policy documents and treaties and change their practices accordingly. It addresses several concerns related to server logs, combined search queries and their storage, and detailed profiling of users.

2. DEFINITION OF A "SEARCH ENGINE" AND BUSINESS MODEL

Generally speaking, search engines are services that help their users to find information on the Web. They can be distinguished according to the different types of data they aim to retrieve, including pictures and/or videos and/or sound or different kinds of formats. A new area of development is search engines that are specifically aimed at building profiles of people based on personal data found anywhere on the Internet.

In the context of the Directive on Electronic Commerce (2000/31/EC) search engines have been denoted as a type of information society service[6], namely information location tools[7]. The Working Party is using this categorisation as the point of departure.

---

3 The Working Group has been initiated by Data Protection Commissioners from different countries in order to improve privacy and data protection in telecommunications and media

4 http://www.datenschutz-berlin.de/doc/int/iwgdpt/search_engines_en.pdf

5 http://www.privacyconference2006.co.uk/index.asp?PageID=3

6 Internet search engines are considered in the European legislation on information society services, defined in article 2 of Directive 2000/31/EC. This article refers to Directive 98/34/EC, which specifies the concept of information society service.

7 See Article 21.2 in connection with Recital 18 of the Directive on Electronic Commerce (2000/31/EC).

The primary focus of the Working Party in this Opinion is on search engine providers who follow the dominant search engine business model based on advertising. This focus includes all the major well known search engines, in addition to specialised search engines such as search engines which focus on personal profiling, and meta search engines that present and possibly regroup the results of other existing search engines. This Opinion does not address search functions embedded on websites for the purpose of searching only the website's own domain.

The profitability of such search engines generally relies on the effectiveness of the advertising that accompanies the search results. Revenues are generated in most cases by a 'pay per click' method. In this model, the search engine charges the advertising company whenever a user clicks on a sponsored link. Much research into the accuracy of search results and advertisements is focused on the right contextualisation. In order for the search engine to produce the desired results and to properly target the advertisements in order to optimise revenues, search engines try to gain as much insight as possible into the characteristics and context of each individual query.

3. WHAT KIND OF DATA?

Search engines process a variety of data[8]. A list of the data involved can be found in the appendix.

Log Files

The log files of specific individuals' use of the search engine service are – assuming they are not anonymised – the most important personal data that are processed by the search engine providers. Data outlining the use of the service can be divided into different categories: namely the query logs (content of the search queries, the date and time, source (IP address and cookie), the preferences of the user, and data relating to the user's computer); data on the content offered (links and advertisements as a result of each query); and data on the subsequent user navigation (clicks). Search engines may also process operational data relating to user data, data on registered users and data from other services and sources such as e-mail, desktop search, and advertising on third party websites.

IP addresses

A search engine provider may link different requests and search sessions originating from a single IP address[9]. It is thus possible to track and correlate all the web searches originating from a single IP address, if these searches are logged. Identification can be improved, when the IP address is correlated with a user unique ID cookie distributed by the search engine provider, since this cookie will not change when the IP address is modified.

The IP address may also be used as location information, even if it may in many cases be inaccurate at present.

---

8 One of the means used by the Article 29 Working Party was the preparation of a questionnaire on privacy policies. The questionnaire was sent to several search engines across member states as well as to several US-based engines. This Opinion partially relies on the analysis of the replies to this questionnaire. The questionnaire is attached to this Opinion, see Annex 2.

9 An increasing number of ISPs distribute fixed IP addresses to individual users.

Web cookies

User cookies are provided by the search engine and stored on the user's computer. The content of the cookies varies from one search engine provider to another. Cookies deployed by search engines typically contain information about the user's operating system and browser, and a unique identification number for each user account. They allow a more accurate identification of the user than the IP address. For instance, if the computer is shared by several users with separate accounts, each user would have his own cookie uniquely identifying him as a user of the computer. When a computer has a dynamic and variable IP address, and cookies are not erased at the end of a session, such a cookie makes it possible to trace the user from one IP address to the next. It can also be used to correlate searches originating from nomadic computers, for instance laptops, since a user would have the same cookie at different locations. Finally if several computers are sharing an Internet connection (e.g. behind a box or a Network Address Translation router), the cookie allows for an identification of individual users on the different computers.

Search engines use cookies (usually persistent cookies) to improve the quality of their service by storing user preferences and tracking user trends, such as how people search. Most browsers are initially set up to accept cookies, but it is possible to reset the browser to refuse all cookies, only to accept session cookies or to indicate when a cookie is being sent. However, some features and services may not function properly if cookies are disabled and advanced features involving cookie management are not always sufficiently easy to configure.

Flash cookies

Some search engine companies install flash cookies on the user's computer. At present, flash cookies cannot be erased simply, e.g. using deletion tools shipped by default with web browsers. Flash cookies have been used, for instance, to backup normal web cookies which can easily be deleted by the users or to store extensive information on user searches (e.g. all the web queries sent to a search engine).

4. LEGAL FRAMEWORK

4. 1. Controllers of user data

4.1.1. The fundamental right - respect for private life

The extensive collection and storage of search histories of individuals in a directly or indirectly identifiable form invokes the protection under Article 8 of the European Charter of Fundamental Rights.

An individual's search history contains a footprint of that person's interests, relations, and intentions. These data can be subsequently used both for commercial purposes and as a result of requests and fishing operations and/or data mining by law enforcement authorities or national security services.

According to Recital 2 of Directive 95/46/EC, "data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals".

Search engines play a crucial role as a first point of contact to access information freely on the internet. Such free access to information is essential to build one's personal opinion in our democracy. Therefore, Article 11 of the European Charter of Fundamental Rights is of special relevance because it provides that *"information should be accessible without any surveillance by public authorities, as part of freedom of expression and information".*

4.1.2. Applicability of Directive 95/46/EC (Data Protection Directive)

In earlier working documents, the Article 29 Working Party has provided clarifications regarding the data protection rules triggered by the logging of IP addresses and the use of cookies in the context of information society services. This opinion will provide further guidance as to the application of the definitions of "personal data" and "controller" by search engine providers. Search engines services can be provided over the internet from within the EU/EEA, from a location outside of the territory of the EU/EEA Member States, or from multiple locations in the EU/EEA and abroad. Therefore, the provisions of Article 4 will also be discussed. Article 4 of the Data Protection Directive addresses the applicability of national data protection law.

Personal data: IP addresses and cookies

In its Opinion (WP 136) on the concept of personal data, the Working Party has clarified the definition of personal data[10]. An individual's search history is personal data if the individual to which it relates, is identifiable. Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address.

The Working Party noted in its WP 136 that*"... unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side",* These considerations will apply equally to search engine operators.

[10] WP 136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

Cookies

When a cookie contains a unique user ID, this ID is clearly personal data. The use of persistent cookies or similar devices with a unique user ID allows tracking of users of a certain computer even when dynamic IP addresses are used[11]. The behavioural data that is generated through the use of these devices allows focusing even more on the personal characteristics of the individual concerned. This is in line with the fundamental logic of the dominant business model.

Controller

A search engine provider that processes user data including IP addresses and/or persistent cookies containing a unique identifier falls within the material scope of the definition of the controller, since he effectively determines the purposes and means of the processing. The multinational nature of the large search engine providers - often with head offices located outside of EEA, services offered worldwide, the involvement of different branches and possibly third parties in the processing of personal data - has given rise to debate about the question who should be considered to be controller with respect to a processing of personal data.

The Working Party would like to stress the difference between the definitions of EEA data protection law and the question whether the law applies in a given situation. A search engine provider that processes personal data, such as logs with personally identifiable search histories, is considered to be the controller of these personal data, regardless of the question about jurisdiction.

Article 4 Data Protection Directive / applicable law

Article 4 of the Data Protection Directive addresses the question of applicable law. The Working Party has provided further guidance regarding the provisions of Article 4 in its "**Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites**[12]". There are two rationales behind this provision. The first is to avoid gaps in and circumvention of the established system of Community data protection. The second is to avoid the possibility that the same processing operation might be governed by the laws of more than one EU Member State. Because of the transnational nature of the data flows induced by search engines, the Working Party specifically addresses both complications.

In the case of a search engine service provider that is established in and provides all of its services from one or more Member States, there is no doubt that its processing of personal data falls within the scope of the Data Protection Directive. It is important to note that in this case, data protection rules are not restricted to data subjects on the territory or of a nationality of one of the Member States.

Where the search engine service provider is a non EEA-based controller, there are two cases in which Community data protection law still applies. Firstly, where the search engine provider has an establishment in a Member State, as in Article 4(1)(a). Secondly,

---

[11] WP 136: "At this point it should be noted that 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."

[12] WP 56, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

where the search engine makes use of equipment on the territory of a Member State, as in Article 4(1)(c). In the latter case the search engine, according to Article 4 (2) has to designate a representative in the territory of that particular Member State.

Establishment on the territory of a Member State (EEA)

Article 4(1)(a) states that a Member State's data protection law should be applied, when certain operations of personal data processing by the controller are carried out "in the context of the activities of an establishment" of that controller on the territory of a Member State. A particular processing operation of personal data should be taken as the starting point. When applied to a particular search engine whose headquarters are located outside of the EEA, the question needs to be answered whether the processing of user data involves establishments on the territory of a Member State.

As the Working Party has already pointed out in its previous Working document[13], the existence of an "establishment" implies the effective and real exercise of activity through stable arrangements and has to be determined in conformity with the case law of the Court of Justice of the European Communities. The legal form of the establishment – a local office, a subsidiary with legal personality or a third party agency – is not decisive.

However, a further requirement is that the processing operation is carried out "in the context of the activities" of the establishment. This means that the establishment should also play a relevant role in the particular processing operation. This is clearly the case, if:

- an establishment is responsible for relations with users of the search engine in a particular jurisdiction;
- a search engine provider establishes an office in a Member State (EEA) that is involved in the selling of targeted advertisements to the inhabitants of that state;
- the establishment of a search engine provider complies with court orders and/or law enforcement requests by the competent authorities of a Member State with regard to user data.

It is the search engine service provider that is responsible for clarifying the degree of involvement of establishments on the territory of Member States when processing personal data. If a national establishment is involved in the processing of user data, Article 4(1)(a) of the Data Protection Directive applies.

Non-EEA based search engine providers should inform their users about the conditions in which they must comply with the Data Protection Directive, whether by establishment or by the use of equipment.

Use of equipment

Search engines that use equipment on the territory of a Member State (EEA) for the processing of personal data also fall under the scope of that Member State's data protection law. A Member State's data protection law still applies where *the controller […] for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.*

[13] WP 56, page 8, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

In terms of the provision of search engine services from outside of the EU, data centres situated on the territory of a Member State may be used for the storage and remote processing of personal data. Other types of equipment could be the use of personal computers, terminals and servers. The use of cookies and similar software devices by an online service provider can also be seen as the use of equipment in the Member State's territory, thus invoking that Member State's data protection law. This issue was discussed in the above mentioned working document (WP56). It stated that "*the user's PC can be viewed as equipment in the sense of Article 4 (1) c of Directive 95/46/EC. It is located on the territory of a Member State. The controller decided to use this equipment for the purpose of processing personal data and, as it has been explained in the previous paragraphs, several technical operations take place without the control of the data subject. The controller disposes over the user's equipment and this equipment is not used only for purposes of transit through Community territory.*

Conclusion

The combined effect of Articles 4 (1) (a) and 4 (1) (c) of the Data Protection Directive is that its provisions apply to the processing of personal data by search engine providers in many cases, even when their headquarters are outside the EEA.

Which national law applies in a certain case, is a matter of further analysis of the facts of that case. The Working Party expects the search engine providers to contribute to this analysis by providing adequate clarification of their role and activities in the EEA.

In the case of multinational search engine providers:

- a Member State in which the search engine provider is established, shall apply its national data protection law to the processing, according to Article 4 (1) (a);
- if the search engine provider is not established in any Member State, a Member State shall apply its national data protection law to the processing, according to Article 4 (1) (c), if the company makes use of equipment, automated or otherwise, on the territory of that Member State[14], for the purposes of processing personal data (for example, the use of a cookie).

In certain cases, a multinational search engine provider will have to comply with multiple data protection laws as a result of the rules regarding the applicable law and the transnational nature of its personal data processing:

- a Member State shall apply its national law to a search engine established outside the EEA if it makes use of equipment;
- a Member State cannot apply its national law to a search engine established in the EEA, in another jurisdiction, even if the search engine makes use of equipment.

[14] The Working Party considers the following criteria to determine the enforceability of Article 4 (1) (c) with regard to the use of cookies. The first is the situation in which a search engine service provider has an establishment in a Member State to which Article 4(1) (a) does not apply, because this establishment does not have a significant impact on the data processing (such as, for example, a press representative). Other such criteria are the development and/or design of country-specific search engine services, the actual knowledge by the online service provider that it is dealing with users that are located in that country, as well as having the advantage of an enduring share of the user market in a particular Member State.

In such cases, the national law of the Member State in which the search engine is established is applicable.

4.1.3 Applicability of Directive 2002/58/EC (ePrivacy Directive) and Directive 2006/24/EC (Data Retention Directive)

Search engine services in the strict sense do not in general fall under the scope of the new regulatory framework for electronic communications of which the ePrivacy Directive is part. Article 2 sub c of the Framework Directive (2002/21/EC), which contains some of the general definitions for the regulatory framework, explicitly excludes services providing or exercising editorial control over content:

"Electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;

Search engines therefore fall outside of the scope of the definition of electronic communication services.

A search engine provider can however offer an additional service that falls under the scope of an electronic communications service such as a publicly accessible email service which would be subject to ePrivacy Directive 2002/58/EC and Data Retention Directive 2006/24/EC.

Article 5(2) of the Data Retention Directive specifically states that "No data revealing the content of the communication may be retained pursuant to this Directive". Search queries themselves would be considered content rather than traffic data and the Directive would therefore not justify their retention.

Consequently, any reference to the Data Retention Directive in connection with the storage of server logs generated through the offering of a search engine service is not justified.

<u>Article 5 (3) and 13 of the ePrivacy Directive</u>
Certain provisions of the ePrivacy Directive such as Article 5(3)(cookies and spyware) and Article 13 (unsolicited communications) are general provisions which are applicable not only to the electronic communication services but also to any other services when these techniques are used.

Article 5(3) of the ePrivacy Directive, to be read in conjunction with Recital 25 of the ePrivacy Directive, addresses the storage of information on the terminal equipment of users. The use of persistent cookies with unique identifiers allows for the tracking and profiling of the use of a certain computer even when dynamic IP-addresses are used. Article 5(3) and Recital 25 of the ePrivacy Directive clearly stipulate that the storage of such information on the terminal equipment of users, i.e. cookies and similar devices (in

short: cookie), must be in accordance with the provisions of the Data Protection Directive. Article 5 (3) of the ePrivacy Directive thus clarifies the obligations regarding the use of a cookie by an information society service, resulting from the Data Protection Directive.

4.2 Content providers

Search engines process information, including personal information, by crawling, analysing and indexing the World Wide Web and other sources they make searchable and thereby easily accessible through these services. Some search engine services also republish data in a so-called 'cache'.

4.2.1. Freedom of expression and right to private life

The Working Party is aware of the special role search engines have in the online information environment. A balance needs to be struck by Community data protection law and the laws of the various Member States between the protection of the right to private life and the protection of personal data on the one hand and the free flow of information and the fundamental right to freedom of expression on the other hand.

Article 9 of the Data Protection Directive aims to guarantee that this balance is struck in the law of the Member States, in the context of the media. In addition, the European Court of Justice has made clear that limits to freedom of expression that might derive from the application of data protection principles, must be in accordance with the law and respect the principle of proportionality[15].

4.2.2 Data Protection Directive

The Data Protection Directive does not contain a special reference to the processing of personal data by information society services that act as selection intermediaries. The Data Protection Directive's (95/46/EC) decisive criterion for the applicability of data protection rules is the definition of the controller, notably whether a certain party "alone or jointly with others determines the purposes and means of the processing of personal data". The question whether an intermediary should be considered to be the controller itself or a controller jointly with others with regard to a certain processing of personal data is separate from the issue of liability for such processing[16].

---

[15] The European Court of Justice has elaborated on the proportionality of the impact of data protection rules, i.e. on freedom of expression in its judgement in the case of Lindqvist v. Sweden, paragraph 88-90.

[16] In some Member States there are special horizontal exceptions ('safe harbors') regarding the liability of search engines ('information location tools'). The Directive on Electronic Commerce (2000/31/EC) does not contain safe harbors for search engines, but in some Member States such rules have been implemented. See 'First report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), 21.11.2003, COM/2003/0702 final.', p. 13.

The principle of proportionality requires that to the extent that a search engine provider acts purely as an intermediary, it should not be considered to be the principal controller with regard to the content related processing of personal data that is taking place. In this case the principal controllers of personal data are the information providers[17]. The formal, legal and practical control the search engine has over the personal data involved is usually limited to the possibility of removing data from its servers. With regard to the removal of personal data from their index and search results, search engines have sufficient control to consider them as controllers (either alone or jointly with others) in those cases, but the extent to which an obligation to remove or block personal data exists, may depend on the general tort law and liability regulations of the particular Member State[18].

Website owners may opt out *a priori* of both the search engine and the caching by using the robots.txt file or the Noindex/NoArchive tags[19]. It is essential that search engine providers respect opt-outs expressed by website editors. This opt-out can be expressed before the first crawling of the website or once it has already been crawled; in that case, updates on the search engine should be carried out as soon as possible.

Search engines do not always limit themselves strictly to an intermediary role. For instance, some search engines store complete parts of the content on the Web - including the personal data in that content - on their servers. Also, it is unclear to what extent search engines are actively targeting personally identifiable information in the content they process. Crawling, analysing and indexing can be done automatically without revealing the presence of personally identifiable information. The format of specific types of personally identifiable information, such as social security numbers, credit card numbers, telephone numbers and e-mail addresses, makes these data easily detectable. But also more sophisticated technology exists and is increasingly being employed by search engine providers, such as facial recognition technology in the context of image processing and image search.

Thus search engine providers may perform value-added operations linked to characteristics or types of personal data on the information they process. In such cases the search engine provider is fully responsible under data protection laws for the resulting content related to the processing of personal data. The same responsibility applies to a search engine that sells advertisement triggered by personal data – such as the name of a person.

---

17 Users of the search engine service could strictly speaking also be considered as controllers, but their role will typically be outside the scope of the Directive as "purely personal activity" (see Article 3 (2) second indent).

18 In some EU Member States data protection authorities have specifically regulated the responsibility of search engine providers to remove content data from the search index, based on the right of objection enshrined in Article 14 of the Data Protection Directive (95/46/EC) and on the e-Commerce Directive (2000/31/EC). According to such national legislation, search engines are obliged to follow a notice and takedown policy similar to hosting providers in order to prevent liability.

19 This may be more than an optional solution. Publishers of personal data need to consider whether their legal basis for publication includes indexing of this information by search engines, and create respective safeguards as necessary, including, but not limited to, use of the robots.txt file and/or Noindex/NoArchive tags.

The caching functionality

The cache functionality is another way in which a search engine provider may go beyond its role as exclusive intermediary. The retention period of content in a cache should be limited to the time period necessary to address the problem of temporary inaccessibility to the website itself.

Any caching period of personal data contained in indexed websites beyond this necessity of technical availability, should be considered an independent republication. The Working Party holds the provider of such caching functionalities responsible for compliance with data protection laws, in their role as controllers of the personal data contained in the cached publications. In situations where the original publication is altered, for example to remove incorrect personal data, the controller of the cache should immediately comply with any requests to update the cached copy or temporarily block the cached copy until the website has been revisited by the search engine.

5. THE LAWFULNESS OF PROCESSING

In accordance with Article 6 of the Data Protection Directive, personal data must be processed fairly and lawfully; they must be collected for specified, explicit and legitimate purposes and not be processed for purposes incompatible with the purposes for which they were originally collected. Moreover, the processed data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. For any personal data processing to be lawful, it needs to satisfy one or more of the six grounds for legitimate processing set out in Article 7 of the said Directive.

5.1. Purposes/grounds mentioned by search engine providers

Search engine providers have generally mentioned the following purposes and grounds for using and storing personal data in their role as controllers of user data.

Improving the service

Many controllers utilise server logs to improve their services and the quality of their search services. In their view, server log analysis is an important tool in refining the quality of searches, results, and advertisements, and also to build new, yet unforeseen, services.

Securing the system

Server logs are said to contribute to keeping search engine services secure. Some search engine providers have stated that log retention can help protect the system from security attacks, and that they require a sufficient historical sample of server log data in order to detect patterns and analyse security threats.

Fraud prevention

Server logs are said to contribute to protecting search engines' systems and users from fraud and abuse. Many search engine providers operate a 'pay per click' mechanism for the advertisements shown. As a drawback, this may lead to a company being unfairly charged if an attacker uses automatic software to click systematically on the

advertisements. Search engine providers devote attention to ensure that this type of behaviour is detected and eradicated.

Accounting requirements are claimed as purpose for services such as clicks on sponsored links, where there is a contractual and accounting obligation to retain data, at a minimum until invoices are paid and the period for legal disputes has expired.

Personalised advertising
Search engine providers seek personalised advertising in order to increase their revenues. Current practices include taking into account history of past queries, user categorisation and geographical criteria. Therefore, based on the behaviour of the user and on his or her IP address, a personalised advertisement can be displayed.

Statistics are collected by some search engines to determine what categories of users access what information online, at what time of the year. This data can be used to improve the service, to target advertisements and also for commercial purposes to determine the cost for a company that wants to advertise its products.

Law enforcement
Some providers state that logs are an important tool for law enforcement to investigate and prosecute serious crimes, such as child exploitation.

5.2. Analysis of purposes and grounds by the Working Party

Generally, search engine providers fail to provide a comprehensive overview of the different specified, explicit and legitimate purposes for which they process personal data. Firstly, some purposes, such as 'improvement of the service' or 'the offering of personalised advertising' are too broadly defined to offer an appropriate framework to judge the legitimacy of the purpose. Secondly, because many search engine providers mention many different purposes for the processing, it is not clear to what extent data are reprocessed for another purpose that is incompatible with the purpose for which they were originally collected.

The collection and processing of personal data may be based on one or more legitimate grounds. There are three grounds which search engine providers may appeal to for different purposes.

- Consent - Article 7 (a) of the Data Protection Directive

Most search engine providers offer both unregistered and registered access to the service. In the latter case, for example when a user has created a specific user account, consent[20] may be used as the legitimate ground for the processing of certain well-specified categories of personal data for well-specified legitimate purposes, including retention of data for a limited period of time. Consent cannot be construed for anonymous users of the service and the personal data collected from users who have not chosen to

[20] Article 2 (h) of the Data Protection Directive "the data subject consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"

authenticate themselves voluntarily. These data may not be processed or stored for any other purpose than acting upon a specific request with a list of search results.

- Necessary for the performance of a contract - Article 7 (b) of the Data Protection Directive

Processing may also be necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This legal basis may be used by search engines to collect personal data that a user voluntarily provides in order to sign-up for a certain service, such as a user account. This basis may also be used, similar to consent, to process certain well-specified categories of personal data for well-specified legitimate purposes from authenticated users.

Many internet companies also argue that a user enters into a de facto contractual relationship when using services offered on their website, such as a search form. However, such a general assumption does not meet the strict limitation of necessity as required in the Directive[21].

- Necessary for the purposes of a legitimate interest pursued by the controller - Article 7 (f) of the Data Protection Directive

According to Article 7(f) of the Directive, the processing could be necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).

Service improvements

Several search engine providers store the content of user queries in their server logs. Such information is an important tool for search providers, allowing them to improve their services by analysing the kind of queries that people make, the way in which they choose to refine those queries and the search results that they choose to follow up. However, it is the opinion of the Article 29 Working Party that search queries do not need to be attributable to identified individuals in order for them to be used to improve search services.

In order to correlate the actions of an individual user (and thus find out, for instance, whether suggestions made by the search engine are helpful), it is necessary only to distinguish one user's actions during a single search query from another's; it is not necessary to be able to identify those users. For instance, a search engine may want to know that User X searched for "Woodhouse" and then chose also to click on results for the suggested spelling variation "Wodehouse", but does not need to know who User X is. Service improvement can therefore not be considered to be a legitimate reason for storing data that has not been anonymised.

---

[21] Article 7 sub (b) of the Directive: "… necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

System security

Search engines may deem the need to maintain the security of their system a legitimate interest and adequate grounds for processing personal data. However, any personal data stored for security purposes must be subject to strict purpose limitation. Therefore, data stored for security purposes may not be used to optimise a service for instance. Search engine providers argue that server logs need to be stored for a reasonable period (the number of months differs from search engine to search engine) in order to enable them to detect patterns of user behaviour and thus to identify and prevent denial of service attacks and other security threats. All such providers should be able to justify comprehensively the retention period they adopt for this purpose, which will be dependent on the necessity to process these data.

Fraud prevention

Search engines may also have a legitimate interest in detecting and preventing fraud, such as 'click fraud', but as with security purposes, the amount of personal data stored and processed, as well as the length of time for which personal data are retained for this purpose, will depend on whether the data are indeed necessary for fraud detection and prevention.

Accounting

Accounting requirements cannot justify systematic logging of normal search engine data in which the user did not click on a sponsored link. The Working Party - based on the information received from search engine providers in reply to the questionnaire - also has serious doubts that personal data of search engine users are really essential for accounting purposes. For a conclusive evaluation, further research would be needed. In any case, the Working Party calls upon search engine providers to develop accounting mechanisms that are more privacy-friendly, for example by using anonymised data.

Personalised advertising

Search engine providers that wish to provide personalised advertising in order to increase their revenues, may find a ground for the legitimate processing of some personal data in Article 7 (a) of the Directive (consent) or Article 7 (b) of the Directive (performance of a contract) but it is difficult to find a legitimate ground for this practice for users who have not specifically signed in based on specific information about the purpose of the processing. The Working Party has a clear preference for anonymised data.

Law enforcement and legal requests

Law enforcement authorities may sometimes request user data from search engines in order to detect or prevent crime. Private parties may also try to obtain a court order addressing a search engine provider to hand over user data. When such requests follow valid legal procedures and result in valid legal orders, of course search engine providers will need to comply with them and supply the information that is necessary. However, this compliance should not be mistaken for a legal obligation or justification for storing such data solely for these purposes.

Moreover, large amounts of personal data in the hands of search engine providers may encourage law enforcement authorities and others to exercise their rights more often and more intensely which in turn might lead to loss of consumer confidence.

5.3. Some issues to be solved by industry

Retention Periods

If the processing performed by the search engine provider is subject to national legislation, it must comply both with the privacy standards and with the retention periods provided for under the legislation of that specific Member State.

If personal data are stored, the retention period should be no longer than necessary for the specific purposes of the processing. Therefore, after the end of a search session, personal data could be deleted, and continued storage therefore needs an adequate justification. However, some search engine companies seem to retain data indefinitely, which is prohibited. For each purpose, a limited retention time should be defined. Moreover, the set of personal data to be retained should not be excessive in relation to each purpose.

In practice, the major search engines retain data about their users in personally identifiable form for over a year (precise terms vary). The Working Party welcomes the recent reductions in retention periods of personal data by major search engine providers. However, the fact that leading companies in the field have been able to reduce their retention periods suggests that the previous terms were longer than necessary.

In view of the initial explanations given by search engine providers on the possible purposes for collecting personal data, the Working Party does not see a basis for a retention period beyond 6 months[22].

However, the retention of personal data and the corresponding retention period must always be justified (with concrete and relevant arguments) and reduced to a minimum, to improve transparency, to ensure fair processing, and to guarantee proportionality with the purpose that justifies such retention.

To that effect, the Working Party invites search engine providers to implement the principle of "privacy by design" which will additionally contribute to further reduce the retention period. In addition, the Working Party considers that a reduced retention period will increase users' trust in the service and will thus constitute a significant competitive advantage.

In case search engine providers retain personal data longer than 6 months, they will have to demonstrate comprehensively that it is strictly necessary for the service.

In all cases search engine providers must inform users about the applicable retention policies for all kinds of user data they process.

Further processing for different purposes

To what extent and how user data are further analysed and whether or not (detailed) user profiles are being created, depends on the search engine provider. The Working Party is aware of the possibility that this type of further processing of user data touches on a core field of innovation of search engine technology and can have a high relevance for competition. Full disclosure about the further use and analysis of user data could also

[22] National legislation may require earlier deletion of personal data

result in increased vulnerability of search engine services to abuse of their services. However, such considerations can not be pleaded as an excuse for not complying with applicable data protection laws of the Member States. Moreover, search engine providers cannot claim that their purpose in collecting personal data is the development of new services whose nature is as yet undecided. Fairness demands that data subjects are aware of the extent to which their private life might be intruded upon when their data is obtained. This will not be possible unless purposes are more precisely defined.

Cookies

Persistent cookies containing a unique user ID are personal data and therefore subject to applicable data protection legislation. The responsibility for their processing cannot be reduced to the responsibility of the user for taking or not taking certain precautions in his browser settings. The search engine provider decides if a cookie is stored, what cookie is stored and for what purposes it is used. Finally, expiration dates of cookies set by some search engine providers seem to be excessive. For instance, several companies set cookies that expire after many years. When a cookie is used, an appropriate cookie lifetime should be defined both to allow an improved surfing experience and a limited cookie duration. Especially in view of the default settings of browsers, it is very important that users are fully informed about the use and effect of cookies. This information should be more prominent than simply being part of a search engine's privacy policy, which may not be immediately apparent.

Anonymisation

If there is no legitimate ground for processing, or for use beyond the well-specified legitimate purposes, search engine providers must delete personal data. Instead of deletion, search engines may also anonymise data, but such anonymisation must be completely irreversible for the Data Protection Directive to no longer apply.

Even where an IP address and cookie are replaced by a unique identifier, the correlation of stored search queries may allow individuals to be identified. For this reason, where anonymisation rather than deletion of data is chosen, the methods used should be considered carefully and performed thoroughly. This might involve the removal of parts of the search history to avoid the possibility of indirect identification of the user who performed those searches.

Anonymisation of data should exclude any possibility of individuals to be identified, even by combining anonymised information held by the search engine company with information held by another stakeholder (for instance, an internet service provider). Currently, some search engine providers truncate IPv4 addresses by removing the final octet, thus in effect retaining information about the user's ISP or subnet, but not directly identifying the individual. The activity could then originate from any of 254 IP addresses. This may not always be enough to guarantee anonymisation.

Finally, log anonymisation or deletion must also be applied retroactively and encompass all of the relevant search engine's logs worldwide.

Data correlation across services

Many search engine providers offer users the option of personalising their use of services through a personal account. Besides search, they offer services such as e-mail and/or other communication tools such as messenger or chat, and social networking tools like

web logs or social communities. Though the range of personalised services might vary, a shared characteristic is the underlying business model and the continuous development of new personalised services.

The correlation of customer behaviour across different personalised services of a search engine provider and sometimes different platforms[23] is technically made easy by the use of a central personal account, but can also be accomplished by other means, based on cookies or other distinguishing characteristics, such as individual IP addresses. For example, when a search engine also offers a service such as 'desktop search', the search engine acquires information about the (contents of) documents a user creates or views. With the help of these data, search queries can be adapted to a more precise result.

The Working Party finds that the correlation of personal data across services and platforms for authenticated users can only be legitimately done based on consent, after the users have been adequately informed.

Registration with a search engine provider, in order to benefit from a more personalised search service, should be voluntary. Search engine providers may not suggest that using their service requires a personalised account by automatically redirecting unidentified users to a sign-in form for a personalised account, because there is no need and thus no legitimate ground for the collection of these personal data other than the informed consent of the user.

Correlation can also be done for non-authenticated users, based on IP address or on a unique cookie that can be recognised by all the different services offered by a search engine provider. Usually this is done in an automatic way, without the user being aware of such a correlation. Covert surveillance of people's behaviour, certainly private behaviour such as visiting websites, is not in accordance with the principles of fair and legitimate processing of the Data Protection Directive. Search engine providers should be very clear about the extent of correlation of data across services and only proceed on the basis of consent.

Finally, some search engine providers explicitly admit in their privacy policy that they enrich data provided by users with data from third parties, other companies that may for example attach geographical information to ranges of IP addresses or websites carrying advertisements sold by the search engine provider[24]. This kind of correlation might be unlawful, if the data subjects are not informed at the time of collecting their personal data

---

23 For example in the case of Microsoft, from the World Wide Web-based search engine to the internet-connected hardware sold for gaming purposes (Xbox).

24 For example Microsoft, in its Microsoft Online Privacy Notice Highlights says: "When you register for certain Microsoft services, we will ask you to provide personal information. The information we collect may be combined with information obtained from other Microsoft services and other companies." URL: http://privacy.microsoft.com/. And about sharing of data with advertising partners Microsoft in its full privacy statement states: "We also deliver advertisements and provide website analytics tools on non-Microsoft sites and services, and we may collect information about page views on these third party sites as well." URL: http://privacy.microsoft.com/en-us/fullnotice.aspx Google in its privacy policy states: "We may combine personal information collected from you with information from other Google services or third parties to provide a better user experience, including customizing content for you." URL: http://www.google.com/intl/en/privacy.html Yahoo! in its privacy policy states: "Yahoo! may combine information about you that we have with information we obtain from business partners or other companies." URL: http://info.yahoo.com/privacy/us/yahoo/details.html

and if they are not granted an easy way of access to their personal profiles and the right to correct or delete certain elements that are incorrect or superfluous. If the processing in question is not necessary for providing the (search) service, the freely given, informed consent of the user would be required for lawful processing.

6. OBLIGATION TO INFORM DATA SUBJECT

Most internet users are unaware of the large amounts of data that are processed about their search behaviour, and of the purposes for which they are being used. If they are not aware of this processing they are unable to make informed decisions about it.

The obligation to inform individuals about the processing of their data is one of the fundamental principles of the Data Protection Directive. Article 10 regulates the provision of this information where data are obtained directly from the data subject. Data controllers are obliged to provide the data subject with following information:

- the identity of the controller and of his representative, if any;
- the purposes of the processing for which the data are intended;
- any further information such as
    - the recipients or categories of recipients of the data;
    - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
    - the existence of the right of access to and the right to rectify the data concerning him.

As controllers of the user data, search engines should make clear to users what information is collected about them and what it is used for. A basic description of the use of personal information should be provided whenever it is collected, even when a more detailed description is provided elsewhere. Users should be similarly informed about software, such as cookies, that might be placed on their computer when they use the website, and how these can be refused or deleted. The Working Party considers that this information is necessary in the case of search engines to guarantee fair processing.

The information that has been supplied by search engines providers in response to the Working Party's questionnaire shows that important differences exist. Some search engines comply with what is specified in the Directive, including links to their privacy policy both from the home page and from the pages generated in a search process and information about cookies. With other search engines, it is very difficult to locate the privacy policy. Users must be able to easily access the privacy policy before conducting any search, including from the search engine home page.

The Working Party recommends that the full privacy policy be as complete and detailed as possible, mentioning the fundamental principles included in data protection legislation.

The Working Party notes that many privacy policies show some deficiencies with regard to the data subjects rights of access or deletion included in Articles 12, 13 and 14 of the Data Protection Directive. These rights are one of the fundamental elements of the protection of the privacy of individuals.

7. RIGHTS OF DATA SUBJECT

Search engines should respect the rights of data subjects to access, and where appropriate to correct or delete information held about them. These rights apply foremost to the data from authenticated users stored by search engines, including personal profiles. However, these rights also apply to non-registered users, who should have the means to prove their identity to the search engine provider, for example, by registering for access to future data and/or with a statement from their access provider about their use of a specific IP address in the past period about which access is requested. When it comes to the content data, search engine providers are generally not to be held primarily responsible under European data protection law.

In 2000, in its Working document "Privacy on the Internet"[25], the Working Party already explained: *"The personalisation of profiles must be subject to the informed prior consent of the individuals. They must have the right to withdraw their consent at any time and with future effect. Secondly, users must, at any time, be given the opportunity to access their profiles for inspection. They must also have the right to correct and erase the data stored."*

When applied specifically to search engines, users must have the right to access any personal data stored about them according to Article 12 of the Data Protection Directive (95/46/EC), including their past queries, data gathered from other sources and data revealing their behaviour or origin. The Article 29 Working Party considers that it is essential that search engine providers provide the necessary means for the exercise of these rights, by means, for instance, of a web based tool that allows registered users direct access online to their personal data and provides the possibility of opposing certain data processing.

Secondly, the right to correct or delete information also applies to some specific cache data held by search engine providers, once these data no longer match the actual contents published on the Web by the controllers of the website(s) publishing this information[26]. In such a situation, upon receiving a request from a data subject, search engine providers must act promptly to remove or correct incomplete or outdated information. The cache can be updated by an automatic instant revisit of the original publication. Search engine providers should offer users the possibility to request removal of such content from their cache, free of charge.

---

25 WP 37, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf

26 The Working Party suggests that webpage editors develop measures to automatically inform search engines of any request they receive to delete personal data.

8. CONCLUSIONS

The internet was devised as an open, global network allowing information to be exchanged. However, it is necessary to strike a balance between the open nature of the internet and the protection of the personal data of internet users. This balance can be found by distinguishing between the two different primary roles of search engine providers. In their first role, as controllers of user data (such as the IP addresses they collect from users and their individual search history), they are to be held fully responsible under the Data Protection Directive. In their second role, as providers of content data (such as the data in the index), generally they are not to be held as primarily responsible under European data protection law for the personal data they process. Exceptions are the availability of a long-term 'cache' and value added operations on personal data (such as search engines aimed at building profiles of natural persons). When providing such services, search engines are to be held fully responsible under the Data Protection Directive and must comply with all relevant provisions.

Article 4 of the Data Protection Directive states that its provisions apply to a controller who has an establishment on the territory of at least one Member State involved in the processing of personal data. The provisions of the Directive may also apply to search engine providers without an establishment on Community territory, if they make use of equipment, automated or otherwise, situated on the territory of a Member State, for purposes of processing personal data.

Based on the above considerations and taking account of the current modus operandi of search engines, the following conclusions can be drawn:

Applicability of EC Directives

1. **The Data Protection Directive (95/46/EC) generally applies to the processing of personal data by search engines, even when their headquarters are outside of the EEA.**

2. **Non-EEA based search engine providers should inform their users about the conditions in which they must comply with the Data Protection Directive, whether by establishment or by the use of equipment.**

3. **The Data Retention Directive (2006/24/EC) does not apply to internet search engines.**

Obligations on search engine providers

4. **Search engines may only process personal data for legitimate purposes and the amount of data has to be relevant and not excessive in respect of the various purposes to be achieved.**

5. **Search engine providers must delete or anonymise (in an irreversible and efficient way) personal data once they are no longer necessary for the purpose for which they were collected. The Working Party calls for the development of appropriate anonymisation schemes by search engine providers.**

6. **Retention periods should be minimised and be proportionate to each purpose put forward by search engine providers. In view of the initial explanations given by search engine providers on the possible purposes for collecting personal data, the Working Party does not see a basis for a retention period beyond 6 months. However, national legislation may require earlier deletion of personal data. In case search engine providers retain personal data longer than 6 months, they must demonstrate comprehensively that it is strictly necessary for the service. In any case, the information about the data retention period chosen by search engine providers should be easily accessible from their homepage.**

7. **While search engine providers inevitably collect some personal data about the users of their services, such as their IP address, resulting from standard HTTP traffic, it is not necessary to collect additional personal data from individual users in order to be able to perform the service of delivering search results and advertisements.**

8. **If search engine providers use cookies, their lifetime should be no longer than demonstrably necessary. Similarly to web cookies, flash cookies should only be installed if transparent information is provided about the purpose for which they are installed and how to access, edit and delete this information.**

9. **Search engine providers must give users clear and intelligible information about their identity and location and about the data they intend to collect, store or transmit, as well as the purpose for which they are collected[27].**

10. **Enrichment of user profiles with data not provided by the users themselves is to be based on the consent of the users.**

11. **If search engine providers provide means to retain the individual search history, they should make sure they have the consent of the user.**

12. **Search engines should respect website editor opt-outs indicating that the website should not be crawled and indexed or included in the search engines' caches.**

13. **When search engine providers provide a cache, in which personal data are being made available for longer than the original publication, they must respect the right of data subjects to have excessive and inaccurate data removed from their cache.**

---

[27] The Working Party recommends a layered model for privacy policy as described in the *WP Opinion on More Harmonised Information Provisions*
(WP 100, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf)

14. Search engine providers that specialise in the creation of value added operations, such as profiles of natural persons (so called 'people search engines') and facial recognition software on images must have a legitimate ground for processing, such as consent, and meet all other requirements of the Data Protection Directive, such as the obligation to guarantee the quality of data and fairness of processing.

Rights of users

15. Users of search engine services have the right to access, inspect and correct if necessary, according to Article 12 of the Data Protection Directive (95/46/EC), all their personal data, including their profiles and search history.

16. Cross-correlation of data originating from different services belonging to the search engine provider may only be performed if consent has been granted by the user for that specific service.

Done at Brussels, on 4 April 2008

For the Working Party
The Chairman
Alex TÜRK

ANNEX 1
EXAMPLE OF DATA PROCESSED BY SEARCH ENGINES & TERMINOLOGY

Query logs	
Search query	The search query entered into the search engine service, usually stored in search engine logs in the form of the URL of the page offered as a result to the query.
IP address	The Internet Protocol address of the user's computer for each entered query.
Date and time	The date and time a specific query was made.
Cookie	The cookie(s) (and/or similar device(s)) stored on the user's computer, including all cookie parameters, such as the value and expiration date. On the server of the search engine, all data referring to the cookie, such as the following information: "cookie/device X has been placed on computer with IP address Y, on date and time Z".
Flash cookie	or "Local Shared Object" is a cookie installed via Flash technology. It cannot currently be simply erased through the browser settings, unlike traditional web cookies.
Referring URL	The URL of the webpage on which the search request was made, possibly a third party URL.
Preferences	Possible specific preferences of the user in advanced service settings.
Browser	Browser details including the type and version.
Operating system	Operating system details.
Language	Language settings of the user's browser, which can be used to infer the language preference of the user.
Content offered	
Links	The links that have been offered to a specific user as a result of a query at a certain date and time. The search engine results are dynamic. To be able to evaluate the results in detail, the search engine provider needs to store data about the specific links and the order in which they have been shown at a certain date and time in response to a specific user query.
Advertisements	The advertisements that have been shown to the user as a result of a specific user query.
User navigation	Clicks by the user on the organic results and advertisements of the search result page(s). This includes the rank of the specific results that have been followed by the user (first link no. 1 was followed, after which the user returned and followed link no. 8).
Operational data	Because of the operational value and use of some of the data described above, for instance for fraud detection, the security/integrity of the service, and user profiling, search engines flag and analyse these data in various ways. For instance, a particular IP address may be flagged as a probable source of query or click spam, a specific click on an advertisement may be flagged as fraudulent, a query may be flagged as relating to information sources on a certain subject.
Data on registered users	A search engine provider may offer users registration for enhanced services. The provider typically processes user account data, such as the login and password of the user, an email address, and any other personal data provided by the user, such as interests, preferences, age, and gender.
Data of other services/sources	Most search engine providers offer other services, such as e-mail, desktop search and advertising on third party websites and services. These services generate user data, which can be correlated and used to enhance existing knowledge about users of the search engine. The user data and possible profiles can also be enriched with data from other sources, such as geo-location data of IP addresses and demographical data.

ANNEX 2

QUESTIONNAIRE FOR SEARCH ENGINES ON PRIVACY POLICIES

1. Do you store data on individual use of your search services?

2. What kind of information do you store/archive in relation to your search services? (e.g. server logs, keywords, search results, IP addresses, cookies, click data, snapshots of websites (caches), etc.)

3. Do you ask for a user's consent (informed consent) for storing the data indicated in your answer to question 2 and if so, how do you ask for it? If not, on what legal basis do you justify the storage of these data?

4. Do you create user behaviour profiles based on the data indicated in your answer to question 2? If so, for which purposes? Which data do you process? Under which identifier (e.g. IP address, user ID, cookie ID) do you store profiles? Do you ask for a user's consent?

5. If you offer other personalised services besides search services, do you share data collected from your search services with these other services, and/or vice versa? If so, please, specify which data.

6. How long do you store the data indicated in your answer to question 2 and for which purposes?

7. What criteria do you consider when determining the storage period?

8. When you store data for a predetermined period, what do you do when that period expires and what procedures are in place in this respect?

9. Do you anonymize data? If so, how do you anonymize it? Is the anonymization irreversible? What information does the anonymized data still contain?

10. Are data accessible to e.g. personnel, or are they processed without human intervention?

11. Do you pass on data to third parties? In which countries? Please, specify for the following categories which kind of data you may share and in which countries:

    - Advertisers

    - Advertising partners

    - Law enforcement authorities (compliance with legal obligations to hand over data in for example court cases

    - Others, please, specify

12. How do you inform users about data collection, data processing and data storage? Do you provide users with comprehensive information on e.g. cookies, profiling, and other tools that monitor website activity? If so, please attach a copy of the information notice, as well as a description of its placement.

13. Do you provide users with the right of access and the right to rectify data or have them altered, erased or blocked? Is it possible to completely opt out of data collection or storage in such a way that no individual data are collected and no traces of the individual user are left on any relevant storage system? Are there any costs associated with the exercise of these rights?

14. Do you apply security measures to data storage? Which ones?

15. Have you notified a national data protection authority in the EEA? If so, please, indicate the authority. If not, please state the reasons why you did not notify.