



Search engine operators and recent WP29 privacy concerns

G. Marcoccio, June 2010

Foreword

At the end of May 2010, WP29¹ sent letters to 3 market-relevant search engine operators with the aim to highlight what are still considered their open issues from the perspective of European provisions on personal data protection and privacy.

The social and economical high values of the services offered by these operators as well as their international scope, render this case an interesting example of the real problems and questions that need to be faced, with due attention in order to balance the impacts for all the involved stakeholders.

What about the EU privacy laws applicability

With the 1/2008 “Opinion on data protection issues related to search engines”², working party WP 29 pointed out several important aspects of this matter, first of all the applicability of the EU directives:

- 95/46/EC³: Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- 2002/58/EC⁴: Directive of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- 2006/24/EC⁵: Directive of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

The question arises from the international scenario of the Search Engine Services (SES), in particular:

- A SES operator can be established or not in EEA⁶ countries
- A SES user can be located everywhere, both in EEA and not EEA countries

taking also in mind that the personal data which are part of the content of a SES service (i.e. the result of a search) can belong to anybody/are located everywhere (again EEA/ not EEA).

¹ This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

² http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf

³ http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>

⁵ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>

⁶ The Agreement creating the European Economic Area (EEA) entered into force on 1 January 1994. It allows the EEA EFTA States (Norway, Iceland and Liechtenstein) to participate in the EU Internal Market without having to join the EU itself. All new relevant Community legislation is dynamically incorporated into the Agreement and thus applies throughout the EEA, ensuring the homogeneity of the internal market.



95/46/EC

The base of reasoning is given by Article 4 of this directive, and the consequent guidance always provided by WP 29 with the WP 56⁷.

The so-called EU privacy directive provides almost two ways in assessing its applicability to the SES context: First one, Article 4(1)(a), is the country of establishment of the data Controller (in our case the SES operator),

Second one, Article 4(1)(c), is the equipment belonging to a SES user, located in EEA, that SES operator uses to provide the service and not only to transit through the EEA territory.

When a SES operator is established in and provides the services from one or more Member State, the directive is applicable without doubts.

When a SES operator is not established in any Member State and, for the purpose of the service provision, processes personal data by means of equipment on the territory of a Member State, then due to Article 4(1)(c) the privacy law of that Member State is to be applied. This case of "equipment" is typically given by the personal computer/mobile of the SES user, equipment where the SES operators install a component (usually cookies) by which personal data of the user are processed to allow provision of the service.

Case by case, further refinements need to be made in order to individuate the complete set of applicable national EU privacy laws (as transposed by the 95/46/EC directive), always on the basis provided by Article 4(1)(a) and Article 4(1)(c), considering that in certain circumstances a SES operator needs to comply with multiple national privacy laws.

In summary:

SES operator established in a:	By the rule:	It applies EU national privacy:
EEA country	Article 4(1)(a)	law where the SES operator is established (*)
NOT EEA country	Article 4(1)(c)	laws of the EEA countries where the SES operator uses equipment to process personal data of the SES users, for the purpose of service provision

(*) as pointed out in Opinion 1/2008 "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. In such cases, the national law of the Member State in which the search engine is established is applicable."

2002/58/EC

In their role of content providers the SES operators are not addressed by this e-privacy directive. Considering that it has recently amended in November 2009 by 2009/136/EC directive, any further consideration at EU national levels needs to be delayed when Members States will adopt by 25 May 2011 the laws, regulations and administrative provisions necessary to comply with this Directive.

WP29 in any case underlines that certain provisions of the e-privacy directive such as Article 5 (3) (cookies and spyware) and Article 13 (unsolicited communications) have a more general applicability (thus including in the scope any other services when these techniques are used), therefore SES operators are required to implement consequent measures .

2006/24/EC

The search queries are considered content rather than traffic data, for this reason the Data Retention does not apply, as clarified in Article 5 (2)"....2. No data revealing the content of the communication may be retained pursuant to this Directive".

⁷ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf



Executive Summary of the WP 29 letters outcomes

- 1) Limit the retention period of personal data,
- 2) Reduce the possibility to identify users in the search logs,
- 3) Develop audit processing involving external and independent auditing entity,

These are the essential issues underlined by WP29 with letters addressed to 3 main SES operators on the market⁸, in order to improve the protection of on line privacy of users.

Limit the retention period of personal data

WP 29 recommends to reduce the data retention period, not exceeding 6 months as indicated in the Opinion 1/2008 with the conclusion #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.”*

The involved SES operators still have different retention policies not completely aligned to the WP 29 requirement. In any case it is to underline that the EU decisions and directives in force do not specify a time limit for this kind of data. Therefore the EU requirement still remains the provision of Article 6 (1)(e) of the privacy directive 95/46/EC⁹, as transposed into the Member States.

Conversely other kinds of data have specific retention period provisions at EU level (for traffic data – directive 2006/24/EC), or directly at national level (for instance in Italy: the system administrators logs¹⁰ and video-surveillance operators logs¹¹).

Reduce the possibility to identify users in the search logs

WP 29 underlines that the measures in place are considered not completely adequate for the purpose. Partial anonymisation of the IP addresses and their correlation with cookies and user identifiers, seems to represent the main problems to fix. In the Opinion 1/2008, the conclusion #5 says:

“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.”

⁸ http://ec.europa.eu/justice_home/fsi/privacy/workinggroup/wpdocs/2010-others_en.htm

⁹ PRINCIPLES RELATING TO DATA QUALITY - Article 6 - 1. “Member States shall provide that personal data must be: (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.”

¹⁰ <http://www.garanteprivacy.it/garante/doc.jsp?ID=1628774>

¹¹ <http://www.garanteprivacy.it/garante/doc.jsp?ID=1712680>



Also in this case, the EU requirement still remain the provision of Article 6 (1)(e) of the privacy directive 95/46/EC, as transposed into the Member States.

Develop audit processing involving external and independent auditing entity

This WP29 request involves several interesting and new aspects.

From the SES users point of view, it would represent an important step ahead for the effectiveness and reliability of the SES privacy and data protection measures implemented. For the market of independent auditing bodies, it provides an important input to enlarge the business and at the same time impulse to achieve an international robust and consolidated standard on privacy and personal data protection sector. Then, positive impact should be expected also in the direction of 'privacy by design', that is in the development and implementation of measures for: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure, taking in mind that *"privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation."*¹²

¹² <http://www.privacybydesign.ca/index.htm>