**28th International Data Protection and Privacy Commissioners' Conference**

**London, United Kingdom 2 and 3 November 2006**

# Resolution on Privacy Protection and Search Engines[1]

## Resolution[2]

Today, search engines have become the keys to cyberspace in order to be able to find requested information on the Internet, and thus an indispensable tool. The increasing importance of search engines for finding information on the Internet increasingly leads to considerable inroads into the privacy of users of search engines.

Providers of search engines have the capability to draw up a detailed profile of the interests of their users[3]. Many IP-logs, especially when combined with respective data stored with access providers, allow for the identification of users. Given that the use of search engines is nowadays common practice among netizens, traffic data stored with providers of popular search engines allow for a detailed profile of interests, thoughts and activities across different sectors (for example work, leisure, but also especially sensitive data about e.g. political opinions, religious beliefs, or even sexual preferences).

Data Protection and Privacy Commissioners have been especially concerned about the possibility to draw up profiles of citizens in the past[4]. Now the technology available on the Internet makes this practice, to a certain extent, technically possible on a global basis.

It is clear that this information is potentially personally identifiable. This not only makes it useful to the search engine providers but also to third parties. For example, a recent example highlighted the interest that law enforcement agencies take in this information: In spring 2006, the US Department of Justice had requested from Google, Inc. millions of its users search requests, in a court case inter alia dealing with protection against online child pornography. Google refused to comply and in the end won the case. Later that year, AOL published a list of nearly 20 Million seemingly anonymised search queries about 650.000 AOL users had punched into AOL's search engine over a three-month-period. According to reports in the press, it was possible to identify single users on the basis of the content of their combined search queries. This list, although quickly withdrawn by AOL recognising that it was an error, had by the time of the withdrawal reportedly been downloaded and re-posted many times, and made available in searchable form on a number of websites.

It has to be noted that not only can traffic data constitute personal information, but so can the content of search queries.

These developments underline that search histories stored by providers of search engines now in many cases may constitute personally identifiable data. Specifically, in cases where operators of search engines are also offering other services leading to the identification of an individual (e.g. e-mail), traffic and content data from

---

[1] This resolution does not address search functions offered by content providers for their own web sites. For the purpose of this resolution, "search engine" shall mean a service for finding resources on the Internet based on user-defined search terms and operating across different web sites.

[2] This resolution does not address the issues raised by the practice of many search engines to store and publish copies of the content of websites, including personal data published on such sites legally or illegally ("caching").

[3] Note that this is in some cases done through the use of persistent cookies.

[4] Cf. e.g. the Common Position on Privacy Protection and Search Engines (first adopted at the 23rd Meeting in Hong Kong SAR, China, 15 April 1998; revised and updated at the 39th meeting, 6-7 April 2006, Washington D.C.) of the International Working Group on Data Protection in Telecommunications; http://www.datenschutz-berlin.de/doc/int/iwgdpt/search_engines_en.pdf. Cf. also CHAPTER 5: SURFING AND SEARCHING of the Article 29 Working Party Working document "Privacy on the Internet" - An integrated EU Approach to On-line Data Protection; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf

searches could be combined with other personally identifiable information derived from those other services during a single session (e.g. based on comparing IP-addresses). The percentage of search history data that can be linked to individuals is likely to further rise in the future due to the uptake of the use of fixed IP numbers in high-speed DSL or other broadband connections where user's computers are "always online". It will further rise once the introduction of IPv6 is completed.

**Recommendations**

The International Conference calls upon providers of search engines to respect the basic rules of privacy as laid down in national legislation in many countries, as well as in International policy documents and treaties (e.g. the United Nations Guidelines concerning Personal Data Files, the OECD Privacy Guidelines, the CoE Convention 108, the APEC privacy framework, and the data protection and privacy directives of the European Union), and to change their practices accordingly as applicable:

1. Among other things, providers of search engines should inform users upfront in a transparent way about the processing of data in the course of using their services.

2. In view of the sensitivity of the traces users leave when using a search engine, providers of search engines should offer their services in a privacy-friendly manner. More specifically, they shall not record any information about the search that can be linked to users or about the search engine users themselves. After the end of a search session, no data that can be linked to an individual user should be kept stored unless the user has given his explicit, informed consent to have data necessary to provide a service stored (e.g. for use in future searches).

3. In any case, data minimization is key. Such a practice would also be beneficial for the providers of search engines in simplifying arrangements for meeting demands for user-specific information from third parties[5].

[5] For the purpose of this resolution, `third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.