International Working Group
on Data Protection
in Telecommunications

675.32.28

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. -

Today, the Internet contains a vast amount of information on almost every topic one can think of. In order to be able to find the requested information on the net, search engines have become an indispensable tool. They are the keys to cyberspace.

With these search engines, it is possible to search for personal data which have been published. The result would be a profile of the network activities of a particular person. Search engines can also be used for "data mining". As the Internet is becoming more and more popular for the exchange of information and other activities (e.g. Electronic Commerce), such activities can cause a threat to privacy.

Furthermore, providers of search engines have the capability to draw up a detailed profile of the interests of their users. 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 will allow for a detailed profile of interests, thoughts and activities across different sectors (for example work, leisure, political opinions, or even sexual preferences).

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

The Working Group has already in the past stressed the data protection and privacy problems related to the use of the Internet and has made recommendations for possible steps to solve these problems. With regard to disclosed or published personal data, the Working Group recalls that personal data which the user has voluntarily made public are still under the protection attached to their nature.

Recommendations

Users of the Internet can also be providers of information. They should be aware that every bit of personal information they publish on the net (e.g. when creating their own homepage, or publish articles in newsgroups) can be used by third parties for profiling.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

For example, messages in news groups or on social networking websites can be indexed and traced by search engines, thus adding information to profiles about who expressed which opinion on which subject. One way to reduce this threat to privacy e.g. when participating in news services could be the use of pseudonyms.

Internet service providers and software manufacturers should therefore offer pseudonym services to their customers. In any case, users should be made aware of the risks they are taking when participating in news services, chatrooms or social networking sites under their real e-mail addresses or even their real names.

Users should have the option to limit the use of their data to certain purposes. They should also be capable of excluding their own personal information (or parts thereof) on the net from being monitored by search engines. This can for example be achieved by defining a “no-robots”-option for a website. However, this feature depends on being observed by the providers of search engine services.

Providers of search engines should inform users upfront in a transparent way about the processing of data in the course of using their services.

They should also provide the data subjects with a means to have their data deleted from (outdated) copies of web pages that they may store (“cache”).

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 the 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 stored which are necessary to provide a service.

In any case, data minimization is key. Such a practice would also be beneficial for the providers of search engines who increasingly have to deal with demands for user-specific information from third parties

To protect the privacy of the user, full application of privacy enhancing technologies is required where possible.