

CLIENT ALERT

Privacy & Data Protection

Jul.09.2008

Other sections of this issue:

[Privacy & Data Protection](#) | [ISP-Liability & Media Law](#) | [Contracts & E-Commerce](#) | [E-Communications & IT](#)

The Article 29 Working Party, the EU advisory body on privacy matters, has issued an opinion on data protection issues related to search engines. The opinion offers some useful clarification on a number of matters that may also be of interest to other online intermediaries such as operators of online communities.

Introduction

Search engines recently came under public scrutiny for their *modus operandi* with personal data. On 4 April 2008 the Article 29 Working Party, the EU advisory body on privacy matters, published its long awaited opinion on data protection issues related to search engines. This opinion offers some useful clarification of a few matters.

Territorial application of European data protection law

In the Article 29 Working Party's view, the European data protection legislation applies to virtually all search engine providers, even to those with no physical operations in the EU. That is because this legislation not only applies to entities processing personal data and having a permanent establishment in the EU, but also to entities which make use of equipment in the EU. The Working Party considers the use of cookies on a European user's PC as use of an equipment inside the EU.

Definition of "personal data"

In line with previous opinions, the Article 29 Working Party adheres to a broad scope for the definition of "personal data". Most information processed by search engines, such as server log files (including actual search queries), IP addresses and cookies, can be related to an identifiable person if they are not anonymized and must therefore be considered as personal data.

Responsibility

Of note is the discussion on the responsibility of search engines over the processing of certain personal data. To the extent that search engine providers act merely as intermediaries, they should not be regarded as the controllers of the processing. However, search engine providers are likely to be controllers when performing value-added operations such as crawling, analyzing and indexing linked to types of personal data on the information they process. When caching websites beyond the time period which is necessary to address the problem of temporary inaccessibility to the website itself, search engine providers will also be controllers. It is clear that this position of the Working Party can also be of interest to online intermediaries other than search engines, for instance operators of online communities based on user-generated input. Such operators may also be considered as mere intermediaries except when performing value-added operations.

Justification for personal data processing

The Article 29 Working Party also restricts the lawfulness of certain purposes for which personal data are being processed by search engines, in particular service improvement and compliance to law enforcement requests. This is because most service improvement is possible without having to analyze personal data, whereas law enforcement requests cannot be used as a reason to store personal data before such a request is made.

Suggested policies

Some issues to be solved by the industry are also advanced, with retention periods, cookies and data correlation services being the most interesting. The Article 29 Working Party's suggested 6 month retention period is significantly lower than the period currently respected by the industry (Google lowered its retention period last year from 24 to 18 months). Expiration dates of cookies are said to be excessive, with some companies setting cookies to expire only after many years. The lack of information with regard to cookies is also addressed. This information should, according to the Working Party, be more prominent than simply being part of a search engine's privacy policy, which may not be immediately apparent. Data correlation (i.e. the offering of other services, such as e-mail, messenger or chat, and web logs or social communities, in addition to search) allowing the provider to obtain more information on users is only lawful when the data subject has been clearly informed and has provided his content thereto. Again, these guidelines may also be of interest to operators of online communities.

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

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Thomas De Meese

Partner – Brussels

Phone: +32.2.282.1842

Email: tdemeese@crowell.com