Brussels, 26 May 2010

Microsoft Corporation
Chief Executive Officer

Subject: Working Party 29 Data Protection Commissioners

Dear,

I am writing to you in my capacity as Chairman of the Article 29 Working Party (hereafter: WP29). On behalf of the data protection authorities in the EU united in WP29, I want to encourage you to continue to show leadership in protecting the online privacy of users of your search engine services. Particular measures include a reduction of the possibility to identify users in the search logs and the creation of an external audit process to reassure users that you are delivering on your privacy promises, i.e. by involving an independent and external auditing entity.

In March 2008, WP29 issued a detailed opinion about search engines[1], explaining and harmonising the specific obligations for search engine providers with respect to the EU data protection directive. Prior to the opinion, WP29 sent a questionnaire to search engine providers. Upon publication of the opinion, leading search engine providers were invited to provide a written response to the opinion, followed by a (closed) hearing in February 2009, attended by a representative of your company and three other search engine providers.

In its opinion, WP29 stressed the sensitivity of personal data related to search queries. We know that Microsoft also shares this concern. As you know an individual's search history contains a footprint of that person's interests, relations, and intentions and should rightly be treated as highly confidential personal data. Pursuant to the data protection directive the retention period should be no longer than necessary for the specific purposes of the processing, after which the data should be deleted. The opinion also specifically addresses the risks of incomplete anonymisation. "*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.*"

In response to the opinion, your company publicly announced a willingness to reduce the retention period of cookies and IP addresses to 6 months, pending on the willingness of other search engines to follow suit. In the same statement your Chief Privacy Officer stressed the

[1] Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, WP148, adopted 4 April 2008, URL: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf

importance of strong anonymisation techniques. "*We believe our approach, which completely deletes all cross-session identifiers, is the way to best anonymise the data*."[2]

After careful analysis of your response, WP29 sent you a public letter applauding your policy to delete IP addresses, instead of attempting to anonymise them. However, WP29 also suggested that you should review your retention policy, to bring it in line with the recommended period of a maximum of 6 months, regardless of competitors .[3]

You have responded on the question of anonymisation by publicly indicating[4] that immediately after a search query, you de-identify cookies by applying a one-way hash. After 6 months you will delete the IP address associated with the search query and after 18 months you will remove the de-identified cookie ID and any other remaining cross session-identifiers.

The policy to delete IP addresses completely after 6 months is a significant improvement. However, in order to be able to point to true privacy protection in this area, you should apply the same procedure to all cookies. According to a technical paper describing the process of de-identification[5], you apply a de-identification procedure and hash to the cookies from registered users after 6 months, but you apparently retain the cookies of unregistered users for a period of 18 months. The word 'anonymous ID' does not seem to be adequate, since it still appears to allow for the cross-matching of search queries for a considerable length of time. Secondly, you have not provided enough information about the techniques of hashing to technically assess the quality of your anonymisation policy.[6] Therefore, WP29 cannot conclude your company complies with the European data protection directive.

WP29 urges you to review your anonymisation claims and make the process verifiable, preferably by developing a credible audit process involving an external and independent auditing entity. The actual techniques of anonymisation deserve an open debate, open to public scrutiny, in light of the expanding body of research on the failures of anonymisation.[7]

Notwithstanding the applicability of the data protection directive as outlined in the opinion, WP29 acknowledges the strong international component of this debate and therefore also raises this issue to a transatlantic level.

To this end, I have shared our concerns with the Federal Trade Commission (FTC). I have asked the FTC to use its authority to examine the compatibility of this behaviour with section 5 of the Federal Trade Commission Act. I have done the same with regard to two other leading search engines.

---

[2] Microsoft press statement 'Microsoft Supports Strong Industry Search Data Anonymisation Standards', 8 December 2008, URL: http://www.microsoft.com/emea/presscentre/pressreleases/TrustworthyComputingPR_081208.mspx

[3] Letter from the Article 29 Working Party addressed to search engine operators Google, Microsoft, Yahoo!, 23 October 2009, URL: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009-others_en.htm

[4] Microsoft, 'Microsoft Advances Search Privacy with Bing', 18 January 2010, URL: http://microsoftontheissues.com/cs/blogs/mscorp/archive/2010/01/18/microsoft-advances-search-privacy-with-bing.aspx

[5] Microsoft corporation, 'Privacy Protections in Microsoft's Ad Serving System and the process of "De-identification"', October 2007, URL: http://download.microsoft.com/download/3/1/d/31df6942-ed99-4024-a0e0-594b9d27a31a/privacy%20protections%20in%20microsoft's%20ad%20serving%20system%20and%20the%20process%20of%20de-identification.pdf

[6] If a single hash is applied to all queries of a particular user, without adding random 'salt', the pattern of all searches can be easily restored, thus leading to great re-identifcation risks.

[7] See ao: Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymization of Large Sparse Datasets', 2008 IEEE symp on security and privacy 111 (5 february 2008), URL: http://userweb.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf and Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (13 August 2009), URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

On behalf of WP29 I also continue to offer assistance to the European Commission in developing and enforcing adequate privacy principles and standards with regard to borderless data processing.

A copy of this letter will be sent to the Chairman of the FTC and to the European Commission Vice-President in charge of Justice, Fundamental Rights and Citizenship.

Sincerely yours,

Jacob Kohnstamm
Chairman