Brussels, 26 May 2010

Yahoo!
CEO Yahoo! Inc.

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 call on you to improve the protection of the online privacy of users of your search engine services. 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. I know that Yahoo also shares this concern. 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 stated "*Last year, we committed to anonymizing the data we collect about your searches after 13 months. We are now reducing our retention time to 90 days with limited exceptions for fraud, security, and legal obligations.*"

[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

After careful analysis of your response, WP29 sent you a public letter welcoming your commitment to a reduced retention period but with suggestions in relation to it and your anonymisation policy.[2]

It is welcomed that you have announced steps to improve your (technical) anonymisation policy, for example by deleting the full IP-address from the first full dataset after 90 days instead of just deleting the last octet.[3]

However, a partial deletion of the personal data contained in search logs does not constitute true anonymisation. Secondly, you have not provided enough information about the techniques of hashing, especially with regard to user identifiers and cookies, to technically assess the quality of your anonymisation policy.[4] 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.[5]

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.

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.

---

[2] 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

[3] Testimony by Anne Toth, Vice President of Policy and Head of Privacy, Yahoo! Inc. before the Joint Hearing of the Subcommittee on Communications, Technology and the Internet and the Subcommittee on Commerce, Trade and Consumer Protection of the Energy and Commerce Committee of the United States House of Representatives on Behavioral Advertising: Industry Practice and Consumers' Expectations, 18 June 2009, URL: http://energycommerce.house.gov/Press_111/20090618/testimony_toth.pdf
"*For example, when we made our data retention policy announcement, our intention was to de-identify IP addresses by deleting only the final "octet" or last set of numbers from the IP addresses. However, we recently decided that it would simplify our process to delete the entire IP address within that 90-day period.*"

[4] 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.

[5] 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

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

Sincerely yours,

Jacob KOHNSTAMM
Chairman