

Google's privacy practices continue to fall short of EU standards

By Spyros Pappas(\*) 9 October 2008

Google has announced with much fanfare that it will reduce the amount of time it stores certain search engine data on users from 18 months to nine months. In an open letter to the Article 29 Working Party (the EU privacy regulators' group), Google touted the change as a significant step "to improve" the company's much-criticised privacy practices, and asserted that the move is "consistent" with the recommendations of the working party.

But upon closer inspection, it appears that Google's search log data reform is not quite as privacy-friendly as one would expect at first glance. It also seems clear that Google - which Privacy International ranked dead last in a study of the data protection practices of leading internet companies - has a long way to go to meet European standards.

Let's begin by considering Google's new search log retention policy. The Article 29 Working Party believes that only a six-month retention policy meets European requirements - not nine months - in the absence of an appropriate justification. In response to Google's announcement, the Chairman of the Working Party, Alex Türk, indicated that to date Google has not provided a sufficient justification.

He also noted that Google's anonymisation mechanisms are "insufficient". Indeed, a report on *CNET* indicates that the anonymisation that Google will undertake at nine months will be even less thorough than the company's current practices (1).

When a user conducts a search with Google, the company reportedly stores three main types of information in a log file: the user's IP address, the search terms and a cookie that identifies each browser that visits a Google website.

After 18 months, Google 'anonymises' the IP address and cookie information from its log files. The IP address is 'anonymised' by removing the final eight digits of the number, while other companies eliminate the entire IP address. Under Google's system, it may still be possible to identify a user by using the IP digits that remain in combination with other information.

The 'anonymisation' that will take place at nine months will be even less robust. According to *CNET*, Google has stated it will remove "some" bits of the IP address, but less than the final eight digits. The full octet will only be deleted at 18 months.

Crucially, cookies will only be deleted at that time as well. The failure to delete cookies means that users can still be easily identified for 18 months, despite the new anonymisation policy.

But Google's anonymisation technique - or lack thereof - is only the tip of the iceberg. As the Article 29 Working Party noted in its response to Google's letter: "Google refuses for the moment to submit to the European data protection law".

Incredibly, despite an extensive business and commercial presence in Europe, Google asserts that the company's European entities do not necessarily fall within the jurisdiction of EU data protection law for purposes of internet search services. Google also continues to assert that the storage of Google's cookie data on the terminal equipment of European citizens does not provide such jurisdiction, despite an Article 29 Working Party opinion to the contrary.

And Google refuses to fully accept that in Europe, IP addresses are very often personal data, subject to strict controls on their collection and processing. This position would prevent Europeans from asserting their rights with respect to such data, such as the right to be notified that it is being processed.

Google's continued indifference to European data protection law comes as the company is rolling out the beta version of its web browser, called Chrome. Experts have already identified serious threats to user privacy in the browser's functions.

When a user types a word or phrase into Chrome's combined web address-search box, the browser sends the user's keystrokes back to Google's servers in real time (ie before the enter button is hit). Google then links this information to the user's IP address. This feature can be deactivated, but only with difficulty.

The German DPA recently launched an investigation into Chrome. As Peter Schaar, Germany's data protection commissioner, noted: "My main concern [with Chrome] is the ability to collect users' web addresses, and therefore your complete surfing on the web could be tracked".

Google claims that its "mission is to organise the world's information". When that information concerns the personal data of European citizens, EU regulators must, like the German DPA, work proactively to ensure that Google respects European rules. While Google likes to talk about its concern for privacy, its actions suggest that continued vigilance is essential.

(\*)Spyros Pappas is founder of Pappas & Associates, a Brussels-based law firm, and a former director-general in the European Commission