COUNCIL OF THE EUROPEAN UNION

Brussels, 28 January 2008

5845/08

DATAPROTECT 3
PE 25

NOTE

from :	General Secretariat of the Council
to :	Delegations
Subject:	Summary of the public seminar on Data protection on the Internet (Google-DoubleClick and other case studies) of the **Committee on Civil Liberties, Justice and Home Affairs (LIBE)** of the European Parliament, held in Brussels on 21 January 2007

The meeting was chaired by Mr CAVADA (ALDE, FR) and Mr LAMBRINIDIS (PSE, EL).

I. First round table: The notion of "personal data" in the Internet framework

Mr HUSTINX, European Data Protection Supervisor, stressed that Community law on data protection applied on the Internet, which had already been discussed in documents published by the Article 29 working group. Considering the definition of personal data, he expressed the opinion that, whenever there was a doubt whether individual persons could be identifiable, the data protection rules should apply.

Ms HARBOUR, Commissioner at the US Federal Trade Commission (FTC), stressing that she was expressing her personal opinion and not speaking in the name of the FTC, commented on the US perspective regarding IP addresses as personal data. She noted the lack of a precise definition of personal data and that there was no consensus on IP addresses. Furthermore, she reported that

Google had refused to turn over search data to the Department of Justice, and that AOL had released search data for research, which the New York Times had been able to reverse-engineer to identify individual persons. She also stated that several search engine firms had modified their retention rules, which she acknowledged as a step into the right direction.

Mr ROTENBERG of the Electronic Privacy and Information Center (EPIC) commented on the Google-DoubleClick merger, stating that it had been approved by the FTC without any privacy safeguards being imposed. He expressed the hope that the European Commission would impose such safeguards. He regretted that traditional competition analysis did not take into account the customers' concerns. He stressed that the Internet advertising market differed from the traditional-media markets in the great amount of information obtained. Therefore, in his opinion, privacy interests of individual persons were concerned. He compared the actual merger case with the intended merger of DoubleClick with Abacus nine years ago, where DoubleClick had promised to use the personal information stored in Abacus' databases only in ways that respected anonymity. He reported that the merger had not in the end taken place.

Mr SINGEWALD, Federation of European Direct & Interactive Marketing (FEDMA), expressed the opinion that IP addresses were personal data for ISPs, but not for marketers. He explained that ISPs could not give out the information needed to link the IP address to a customer, because if they did they would be breaking the law. Therefore, in his opinion, there was no reasonable means for a marketer to identify the owner of an IP address, which was consequently not personal data for him.

Mr FLEISCHER, Global Privacy Counsel, Google, regretted that people took the privacy debate and turned it into a competition review. He welcomed the fact that the FTC had refused to do this and had stated that imposing privacy on one company alone would risk infringing competition. Concerning IP addresses, he expressed the opinion that this depended on the context. In his opinion, an IP address did not mean for any website on the planet that they could identify a human being. He called for global privacy standards, stating that rules on Internet privacy could not be different between Europe and the US.

Mr MYRUP KRISTENSEN, EU Internet Policy Director, Microsoft Europe, stated that the question was not simply one of defining personal data, but also of what could be done with it. He stated that for Microsoft, the concepts of transparency and consent in security were the key. For him, it was most important that consumers were informed about what was going on.

Mr SCHAAR, Chairman of the Article 29 Committee, called for a new discussion on data protection. He stated that data protection served to protect real persons. Wherever the link between a service and the person making use of this service was possible, this was personal data. He added that one also had to take into account the capacity of services to exchange the data obtained. He noted that film industry wanted to identify copyright law violators by recording their IP addresses. Therefore, it was in his opinion impossible to rule out the possibility that IP addresses could be linked to individual persons. This meant for him that, as it was possible to relate them to individual persons, IP addresses should always be considered personal data.

Mr HEUREUX, Internet Advertising Bureau Europe (IAB Europe), noted the rapid development of the Internet advertising industry. He stated that freedom of expression over the Internet, via websites, blogs etc, was only possible thanks to the funding of advertising. He underlined that, compared to traditional advertising, Interned advertising was targeted advertising, which meant a more relevant, less irritating advertising for consumers.

Mr VARVITSIOTIS regretted that the industry's representatives did not comment on the growing concern about data protection issues, mentioning the recent issues of discs with personal data getting lost in the UK.

Ms IN 'T VELD stressed the need for cross-Atlantic cooperation on the issue. She noted the growing concern not only about industry use of personal data, but also about the use that government bodies could make of it if industry was giving out the data.

Mr ROTENBERG noted that privacy had been an issue in the US Congress debate, which had considered that the FTC had competence to consider privacy. Therefore, he had been surprised that the FTC had decided that they did not have a mandate for this. He wished that the IP address was not personally identifiable, but according to him this was not the case. He added that there were

hundreds of companies that offered commercial identification of IP addresses and that moving to IPv6 would make them even more identifiable.

Mr FLEISCHER underlined that Ms Harbour was the only out of five Commissioners who had been in favour of taking into account data protection. He added that Google responded to government requests if they were issued in a valid legal process, which was different in every country. He explained a case from last year where Google had taken to court a government request for millions of addresses. He added that Google was the only one of 34 companies concerned that had taken the request to court. He stressed that Google anonymized server logs after 18 months, which meant that it was not even possible to release the data after that time.

Ms HARBOUR agreed that the FTC did not consider the issue of privacy for the merger, explaining that the other Commissioners had taken a traditional point of view. She declared that she remained concerned that the traditional analysis failed to capture the interests of all parties implied, as consumers did not have a business relationship with Google or DoubleClick.

II. Second Round Table: How the industry can minimise the threat for the protection of data when delivering services on Internet (notably via search engines)

Mr LAMBRINIDIS asked Mr Fleischer why Google did not have a big button on the web site allowing for an opt-in for collecting personal data.

Mr FLEISCHER declared that consumer trust was crucial for Google, but called for these issues to be dealt with across the world, not just in one company. He mentioned transparency and choice as the values of Google and explained that Google had released a series of videos on how to use privacy settings. He added that people liked simplicity and choice better than a 7-page privacy policy. Concerning server logs, he stated that they were needed to protect the system from hackers and from click fraud of the advertising system, but also as a record for their business. But he added that Google had reduced the lifetime of their cookies from 30 to 2 years. Stressing the importance of advertising for the Internet, he explained that ads on Google were targeted on search terms, the language settings of the browser and the geographic location as defined by the IP address. Concerning the DoubleClick merger, he stated that Google was new to the business of third party ad serving and wanted to buy DoubleClick for that reason, not in order to merge the databases. He

added that DoubleClick customers' data were owned by the customers, and that Google would remain bound by these contracts.

Mr MYRUP KRISTENSEN acknowledged that the EU had strong data protection rules and described it as a challenge to determine how they applied in particular settings. For him, this was also an opportunity to gain consumer trust. He named transparency, consent and control as Microsoft's principles on data protection. He mentioned the layered approach that helped to avoid the problem of information overload. Concerning data retention, he stated that server logs were anonymised after 18 months, adding that this retention period of 18 months wasnecessary. He stressed the importance of complete anonymisation, including the removal of IP addresses, and added that Microsoft participated in the Safe Harbour System.

Ms KUTTERER from the European Consumers' Organisation BEUC stated that people were not aware of data protection issues. She noted that DoubleClick did not recognize IP addresses as identifiable data and asked how the opinion of the Article 29 Committee on this could be enforced. She went on to say that much more data was collected through services interconnected with search engines, in particular personalised services. Privacy policies were not sufficiently made clear. She saw no need for self-regulation, as there were sufficiently strong laws which just had to be enforced.

Ms NAS of the Dutch Data Protection Agency saw a radical shift in public perceptions as to what was private and what was public. She stated that the data retention directive was not applicable to search engines. She explained that a task force was working on recommendations for search engines, which had not yet been adopted by the plenary. But she agreed that IP addresses should also be considered personal data, because they were used to discriminate between different users. She insisted on the importance of search engines gaining the trust of their users. In her opinion, the privacy directive was adequate, in that it provided a clear, useable framework. For her, it was not for the data protection authorities to consider the consequences of a merger, but for the companies themselves to continue to comply with data protection rules. She also called for adequate enforcement powers of all data protection authorities.

Mr LOMBARTE from the Spanish Data Protection Agency presented an analysis of data protection in search engines conducted by the Spanish Data Protection Agency. In the light of that analysis, he called for more information to be provided to individuals whose data was going to be processed and a guaranteed and effective right to access and correct this information. He also considered it necessary to set a time limit for storage of personal data on the Internet.

Ms HARBOUR reported some conclusions of an FTC workshop on behavioural advertising, namely the relative invisibility of behavioural advertising and the need for transparency and consumer trust, as well as concerns about the data falling into the wrong hands. She then proposed a series of principles. Firstly she proposed a requirement of transparency and consumer control through a prominent statement on every website that used targeted advertising. Furthermore, she called for reasonable data security and retention no longer than for business needs. Finally, she considered express consent necessary for changes in the use of data, and for obtaining or using sensitive data. She added that the FTC was considering whether the use of sensitive data should be prohibited altogether.

Mr CAVADA asked if the content of emails were scanned.

Ms HARBOUR replied that the FTC did not scan emails, as it was only a civil authority.

Mr FLEISCHER answered that Google scanned email messages in order to filter spam and viruses, but also to target adverts based on the content of the messages.

Mr ROTENBERG highlighted this difference between scanning messages to fight against spam and viruses and the analysis of the content for advertising purposes.

Mr SCHAAR drew attention to the content stored in cookies, he proposed limiting the duration of their storage in the default settings of browsers as a way to solve this problem.

Ms IN 'T VELD reacted to Ms NAS by saying that competition and privacy were linked because consumers could exercise their powers to obtain better privacy only if there was enough competition.

Mr COELHO expressed the opinion that legislative measures should be taken to make sure that IP addresses were considered personal information.

Mr MYRUP KRISTENSEN explained that Microsoft did not scan emails. Furthermore, when creating an account, two user profiles were created: one with personal information such as the name, the other one without personal information, which was used for targeting ads.

III. Third Round Table: How the EU legislation can be strengthened, as well as the security of networks, the international cooperation and the growth of the internet services market

A representative of the Commission DG Information Society & Media explained the Directive on Privacy and Electronic Communication (e-Privacy Directive), a part of the regulatory framework for electronic communications. He said that most of the provisions related to the obligations of providers of communications, networks etc. - the same scope as the Data Retention Directive. These rules did therefore not apply to search engines. But the e-Privacy Directive also contained some broader obligations. He stated that several proposals were aimed at increasing privacy, such as the obligation to inform the consumer when a breach of security has occurred that compromises personal data. He also mentioned clarifications concerning the handling of spam and spyware.

Ms HARBOUR detailed the FTC's privacy work, mentioning domestic enforcement actions, cross-border cooperation following the 2006 US Safe Web Act and the APAC cross-border privacy rules package that would, according to her, develop into a cross-border privacy system.

Mr ESTERLE of the European Internet Safety Agency (ENISA) presented the work of his agency, supporting the authorities by providing information. Amongst other aspects, he mentioned recommendations on the use of social networking and a survey on spam. He confirmed that in his opinion, an IP address was personal data because of the discriminatory implications that it might have on the personal life of the subject. Furthermore, he addressed the issue of certification schemes, on which he considered that there was still much to be done.

Ms KUTTERER, speaking of the relationship between privacy and security, was critical about how industry used security as an excuse for the use of private data. She recalled the information asymmetry between industry and consumers. For her, it was also a liability issue; she welcomed a Commission proposal that would lead to better enforcement. In this context, she also mentioned possible group actions. Finally, she called for a comprehensive security breach information law.