

**Statement of Thomas Myrup Kristensen
EU Internet Policy Director, Microsoft Europe**

**Before the
Committee on Civil Liberties, Justice, and Home Affairs
European Parliament**

**“Data Protection on the Internet
(Google-DoubleClick and other case studies)”
21 January 2008**

Thank you for this opportunity to provide Microsoft’s perspective on the important data protection issues presented by advertising on the Internet. We appreciate the initiative the LIBE Committee has taken in holding this hearing. We are also fully committed to working collaboratively with institutions globally to ensure that the concepts of transparency, consent and security -- which are the core principles of Microsoft’s approach to privacy -- are brought to bear to the full benefit of consumers.

Opportunities and Challenges in the Online World

Much is at stake with respect to the issues we will be considering today. Online advertising has become the very fuel that powers the Internet and drives the digital economy. Today, many websites are able to offer their content and services online for free, precisely because of the income they derive from advertising. Simply stated, the Internet would not be the diverse and useful medium it has become, without advertising.

At the same time, online advertising presents challenges and risks. The ability to target online ads depends on information that companies collect from or about Internet users. Needless to say, much of this information may be viewed as personal.

Fortunately, Europe has erected strong legal safeguards, indeed, among the strongest in the world, in the form of data protection rules to protect individuals' privacy. The EU rules are based on long established principles enshrined in the European Convention on Human Rights and, more specifically, the Council of Europe Convention on the protection of personal data.

Transparency of data gathering practices, and proportionality of the data gathered in relation to its purpose and use, are cornerstones of the EU regime. These principles are, of course, expressed in somewhat general terms. They are intended to apply in a wide variety of contexts, both off line and on line. Thus, an important challenge is determining exactly how the rules should apply in a particular setting.

We at Microsoft do not see this only as a challenge. It is also an opportunity to think creatively about how we can build consumer trust. After all, data protection and privacy are about consumer trust. Microsoft has a long-held belief that our customers should be in control of their information, and it is this belief which guides the design of all our products and services.

Some have called for new international standards of online privacy. Others have expressed concern that this could be a diversion. While we are eager to work collaboratively on all fronts, we believe the first priority should be to honor the letter and the spirit of the rules already in place, and, where possible, to develop best practices that exceed those norms.

Ultimately, this is the responsibility of each of us as individual companies. We must each nourish a culture within our companies that truly values and respects privacy. In that spirit, Microsoft was one of the first companies to appoint a chief privacy officer, an action we took nearly a decade ago, and we currently employ over 40 employees who focus on privacy full-time, and another 390 who focus on it as a part of their jobs.

We have devoted considerable time, energy, and resources to the development of privacy-related standards that serve as a practical guide to our handling of personal data. Last July, we

announced additional privacy principles related to search and online advertising, and I would now like to take a moment to share them with you. I will also describe some of the specific practices that illustrate how these principles work in the ‘real world’. We have also included the full text of our principles in Appendix I to the written version of this statement submitted to the Committee.

Microsoft’s Core Online Privacy Principles

Microsoft’s core privacy principles are based on three key concepts: transparency, consent and security. They embrace user control, search data anonymization, data protection, legal compliance and industry best practices.

Our first core principle concerns transparency. We have redoubled our efforts to provide users with clear notice about our policies and practices so that they can make informed choices. We were one of the first companies to develop a so-called “layered” approach to privacy notification, in which users can click on links to obtain more detailed information about a company’s privacy practices. This helps avoid the problem of information overload, while enabling consumers to be fully informed. To illustrate this, we have included screen shots in Appendix II to the written version of this statement submitted to the Committee.

The first layer of our privacy policy provides a clear statement of the key information our customers need to understand Microsoft’s practices from the very beginning – including a statement that data may be used for the display of personalized content and advertising. Additionally, our Online Privacy Statement is readily accessible from every page of each major online service that we operate. Once again, we have included screen shots in Appendix II to illustrate.

Our second core principle involves user control. This is critical. Currently, we are developing new technologies that will dramatically enhance such control, for example, by allowing signed-

in users to control personalization using their search history. Similarly, when we begin to offer advertising services to third party websites, we will comply with the principles of the Network Advertising Initiative by allowing users to opt-out altogether from behavioral ad targeting by Microsoft.

Another core Microsoft privacy principle concerns security and minimization by design. In other words, we design our systems and processes in ways that minimize, from the outset, their privacy impact while promoting security.

For example, we use encryption technology (known as a one way cryptographic hash) to store search terms separately from account holders' personal information, such as name, email address, and phone number. We have also designed our online ad platform to only use data for ad targeting that does not personally and directly identify individual users.

Microsoft invests heavily in protecting all of our online services from unauthorized access, attacks and other malicious activity. These measures include vigorous physical as well as virtual measures to keep data safe, detailed data protection and security plans, third party audits, code reviews, and advanced intrusion detection, to name just a few of the elements.

Related to our core principles of transparency, control, and security is the important issue of data retention. We have implemented specific retention policies with respect to search query data, and we currently anonymize all such data after 18 months, unless we receive user consent for longer retention.

We believe that 18 months is the minimum necessary in current circumstances for the security, integrity, and relevance of our services. However, we have taken a very strict approach to anonymizing search terms by irreversibly removing the entire IP address and all other cross-session identifiers, such as cookies and other machine identifiers, from search terms. This renders that information truly anonymous. In terms of the impact on user privacy, complete

and irreversible anonymity is the most important point here – more impactful than whether data is retained for 13 vs. 18 vs. 24 months.

Finally, we are committed to complying not only with our legal obligations but also with industry best practices in all of the markets in which we operate. We participate in the safe harbor framework regarding the collection, use, and retention of data collected from European residents. We also adhere to the standards set forth in the Organization for Economic Cooperation and Development (OECD) privacy guidelines, and, as we begin to offer advertising services on third party websites, we plan to follow applicable principles of the Network Advertising Initiative.

These principles build on our other privacy efforts, including our support for comprehensive privacy legislation in the United States and our release of privacy guidelines to help developers build meaningful privacy protections into their own software programs. We will also continue to make significant investments in data protection in terms of dedicated personnel, training, and building robust privacy standards into our product development cycles and other business processes.

The bottom line is this. Data protection is a continuous journey, not a single destination. We can and will continue to improve our privacy measures as we seek to develop and implement new protections in the context of complex, evolving technologies. But make no mistake. Protecting privacy is a core value of Microsoft's culture, and we are committed to working hard to bring the benefits of transparency, consent and security to the protection of consumers' data and privacy online.