

Appendix I to the Statement of Thomas Myrup Kristensen
EU Internet Policy Director, Microsoft Europe

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

21 January 2008

Microsoft's Privacy Principles for Live Search and Online Ad Targeting

23 July 2007

Microsoft's Privacy Principles for Live Search and Online Ad Targeting represent the continuing evolution of Microsoft's long-standing commitment to privacy. They build on our existing policies and practices, as reflected in our privacy statements. They also complement our other privacy efforts, such as the public release of our Privacy Guidelines for Developing Software Products and Services and our work to advocate for comprehensive federal privacy legislation in the US and strong public policies worldwide to protect consumer privacy. Some parts of these principles reflect current practices, while other aspects describe new practices that will be implemented over the next 12 months.

In addition to guiding our own practices in the areas of Live Search and online ad targeting, we hope that these principles will be even more valuable in helping to advance an industry dialogue about the protection of privacy in these areas. We also recognize that these are dynamic technologies that are rapidly developing and changing. As such, we will continue to examine and update our privacy approach to ensure that we are striking the right balance for our customers.

Principle I: User Notice

We will be transparent about our policies and practices so that users can make informed choices. For example:

- Our current Microsoft Online Privacy Statement provides clear disclosures in an easy to navigate format that is readily accessible from every page of each major online service that we operate.
- We will regularly update the Microsoft Online Privacy Statement to maintain transparency as our services evolve or our practices change.
- In addition, we will shortly update our privacy statement to provide more detail on online advertising and search data collection and protection.

Principle II: User Control

We will implement new privacy features and practices as we continue to develop our online services.

For example:

- We will continue to offer controls that help users to manage the types of communications they receive from Microsoft.
- Once we begin to offer advertising services to third party websites, we will offer users the ability to opt-out from behavioral ad targeting by Microsoft's network advertising service across those websites, in conformity with the Network Advertising Initiative (NAI) Principles.

- We will continue to develop new user controls that will enhance privacy. Such controls may include letting individuals use our search service and surf Microsoft sites without being associated with a personal and unique identifier used for behavioral ad targeting, or allowing signed-in users to control personalization of the services they receive.

Principle III: Search Data Anonymization

We will implement specific policies around search query data, be explicit with users about how long we retain search terms in an identifiable way, and inform users of when and how we may “anonymize” such data. Specifically:

- We will anonymize all Live Search query data after 18 months, unless we receive user consent for a longer time period. This policy will apply retroactively and worldwide, and will include irreversibly removing the entirety of the IP address and all other cross-session identifiers, such as cookie IDs or other machine identifiers, from the search terms.
- We will ensure that any personalized search services involving users choosing a longer retention period are offered in a transparent way with prominent notice and consent.
- We will follow high standards for protecting the privacy and security of the data as long as it is retained, as described in Part IV below.

Principle IV: Minimizing Privacy Impact and Protecting Data

We will design our systems and processes in ways that minimize the privacy impact of the data we collect, store, process and use to deliver our products and services. For example:

- We will store our Live Search service search terms separately from account information that personally and directly identifies the user, such as name, email address, or phone numbers (“individually identifying account information”). We will maintain and continually improve protections to prevent unauthorized correlation of this data. Moreover, we will ensure that any services requiring the connection of search terms to individually identifying account information are offered in a transparent way with prominent notice and user consent.
- We have also designed our online ad targeting platform to select appropriate ads based only on data that does not personally and directly identify individual users, and we will store clickstream and search query data used for ad targeting separately from any individually identifying account information, as described above.
- We will continue to implement technological and process protections to help guard the information we collect and maintain.

Principle V: Legal Requirements and Industry Best Practices

We will follow all applicable legal requirements as well as leading industry best practices in the markets where we operate. For example:

- We adhere to the standards set forth in the Organization for Economic Cooperation and Development (OECD) privacy guidelines.
- We follow the Online Privacy Alliance (OPA) guidelines.
- We are a member of the TRUSTe Privacy Program.
- We abide by the safe harbor framework regarding the collection, use, and retention of data from the European Union.
- As we begin to offer advertising services on third party websites, we plan to follow applicable Network Advertising Initiative (NAI) Principles, for example:
 - We will give users the opportunity to opt out of behavioral targeting on third party websites (including the delivery of behaviorally targeted ads on third party websites and the usage of data collected on third party websites for behavioral targeting).
 - We will not associate Personally Identifiable Information with clickstream data collected on third party websites without user notice and consent.