Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft®

August 15, 2008

The Honorable John D. Dingell, Chairman
Committee on Energy and Commerce
2328 Rayburn House Office Building
Washington, DC 20515-2215

The Honorable Joe Barton, Ranking Member
Committee on Energy and Commerce
2109 Rayburn House Office Building
Washington, DC 20515-4306

The Honorable Edward J. Markey, Chairman
Subcommittee on Telecommunications and the Internet
2108 Rayburn House Office Building
Washington, DC 20515-2107

The Honorable Cliff Stearns, Ranking Member
Subcommittee on Telecommunications and the Internet
2370 Rayburn House Office Building
Washington, DC 20515-0906

Dear Chairman Dingell, Ranking Member Barton, Chairman Markey, and Ranking Member Stearns:

Thank you for your letter that raises important privacy issues presented by advertising on the Internet. Microsoft has a deep and longstanding commitment to consumer privacy issues, and we welcome the opportunity to describe the way we protect the privacy of individuals online.

There are a variety of online advertising business models, and consequently a variety of ways in which data can be collected about users to serve tailored ads on the Internet. As we understand, the Committee has focused on a relatively new business model where ads are tailored based on information about users' online activities obtained through so-called "deep packet inspection" through a network operator or Internet service provider. This involves the collection of data from potentially all web sites and services that a consumer uses. **To be clear, Microsoft does not engage in deep packet inspection.**

Thus, our answers to the Committee's questions are based on our activities in the more traditional advertising models – specifically, in our roles as an online search provider and as an ad network. The data collection in these cases can be thought of in the following two ways. First, users reveal information about what they are looking for when they search online, and ads can be targeted to their search queries. Second, advertising networks enter into agreements with websites that allow them to display ads on their sites; to deliver and tailor those ads to users' interests, data is gathered about the pages users view and the links users click on within those sites. In both of these models, data is collected about users in connection with displaying ads to them. This means that, in general, the entity with the largest market share in delivering search and non-search ads will also collect the most data about users.

We recognize that the collection of data to serve ads online has implications for consumer privacy. For this reason, Microsoft has encouraged the Federal Trade Commission to develop comprehensive industry self-regulatory principles that impose increasing notice and consent obligations depending on the type of online advertising activity involved. In our opinion, entities that collect any information about users to serve ads online should be transparent about their activities and protect the data they maintain; entities that profile visitors' activity on unrelated third-party sites for the purpose of offering more relevant ads should also offer consumers a robust choice about the use of their information for such purposes; and entities that seek to use sensitive personally identifiable information to tailor ads, should obtain affirmative opt-in consent.

Microsoft believes that strong privacy protections are not only compatible with bringing the benefits of online advertising to consumers, advertisers and publishers, but are essential to ensuring the success of this important business model. If consumers feel that Internet companies are not protecting their privacy, the Internet's ability to serve as an engine of economic growth will be threatened. This means that Microsoft, and all companies operating online, must adopt meaningful privacy practices that build trust with consumers. In this regard, Microsoft has taken more concrete steps than any of its peers to protect the privacy and security of consumers. For example:

- Meaningful Online Advertising Principles. In July 2007, Microsoft announced five fundamental privacy principles for online search and ad targeting. These principles, which we have attached, include commitments to user notice, user control, search data anonymization, security, and best practices. *See* http://www.microsoft.com/privacy. We also have released a set of privacy guidelines designed to help developers build meaningful privacy protections into their software programs and online services. *See* http://www.microsoft.com/privacy.

- Clear and Upfront User Notice. Microsoft was one of the first companies to develop so-called "layered" privacy notices that give clear and concise bullet-point summaries of our practices and direct users to a place where they can find more information. We post a link to this user-friendly privacy notice on every one of our web pages.

- Robust User Control. Microsoft has implemented a robust method to enable users to opt out of behavioral advertising, highlighted on the first layer of our privacy notice. Specifically, users can tie their opt-out choice to their Windows Live ID so their choice will be effective across multiple computers without any additional effort on the user's part. This method is also more persistent – for example, deleting cookies will not erase consumer's opt-out selection. *See* http://www.microsoft.com/privacy.

- Unique Steps To De-Identify Data. Microsoft is unique in our use of a technical method (known as a one-way cryptographic hash) to separate records of search terms and browsing behavior from records that include account holders' personal information, such as name, email address, and phone number, and to keep them separated in a way that prevents them from being easily recombined. We have also relied on this method to ensure that we use only data that does not personally identify individual consumers to serve ads online. A white paper, "Privacy Protections in

Microsoft's Ad Serving System and the Process of "De-identification," provides additional detail on our practices and is publicly available at http://www.microsoft.com/privacy.

- Strict Search Data Anonymization. Microsoft's policy is to anonymize its search log data after 18 months, which we believe is an appropriate timeframe in our circumstances to enable us to maintain and improve the security, integrity and quality of our services. In addition, unlike others, we irreversibly remove the *entire* IP address and other cross-session identifiers, such as cookies and other machine identifiers, from search terms after 18 months.

- Dedicated Privacy Personnel and Processes. 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 400 who focus on it as part of their jobs. We have made significant investments in privacy in terms of dedicated personnel and training and by building robust privacy standards into our product development and other business processes.

- Consumer Education and Private-Public Sector Partnerships. Microsoft educates consumers about ways to protect themselves while online, and we have worked closely with industry members and law enforcement around the world to identify security threats, share best practices, and improve our coordinated response to privacy, security and other Internet safety issues.

- Support for Comprehensive Privacy Legislation. Microsoft was one of the first companies to advocate for comprehensive federal privacy legislation in the United States.

With this background, please find below our responses to the specific questions you have asked.

1. Has your company at any time tailored, or facilitated the tailoring of, Internet advertising based on consumers' Internet search, surfing, or other use?

Yes , we display relevant advertising based upon consumers' using our Internet search service or browsing web sites owned by Microsoft or our specific advertising partners. As noted above, we are not engaged in so-called "deep packet inspection" or any other tailoring of advertising based on users' online behavior obtained through a network operator or an Internet service provider.

2. Please describe the nature and extent of any such practice and if such practice had any limitations with respect to health, financial, or other sensitive personal data, and how such limitations were developed and implemented.

We do not collect or use sensitive personal information to deliver advertising to users, and we believe companies should obtain opt-in consent before using such data for such purpose.[1] We have incorporated other privacy protections into our online advertising business that go beyond what others in industry have done. For example:

[1] In our comments to the Federal Trade Commission, we have proposed that an opt-in standard apply to the use of sensitive personally identifiable information for the purpose of ad targeting. *See* http://www.ftc.gov/os/comments/behavioraladprinciples/080411microsoft.pdf.

- We are very transparent with consumers about the data we collect and how we use it to deliver relevant ads online, as we explain further in our response to Question # 6 below.

- When we entered the business of providing online ads for web sites other than our own, we began work on developing a robust mechanism to give consumers the ability to opt out of receiving relevant advertisements from Microsoft. The functionality of our opt-out choice mechanism is industry-leading, as described in further detail in our response to Question # 7.

- We employ a variety of protections to the data we collect, including using only information that does not directly and personally identify individual consumers to serve advertisements online, as further described in our response to Question # 10.

As background, before 2006, we served ads only on our own websites, and we developed capabilities to target those ads based on the data users directly provided and the pages they viewed or other activities on our sites. In late 2006, we began to offer our ad platform as a service to others, which enabled us to deliver ads and collect page-view information on our advertising partners' websites as well as our own, thereby becoming what is generally referred to as an "ad network." Our investment and activity in this area was accelerated by our acquisition of aQuantive in early 2007.

From the beginning, as we have moved into the online ad business, and have developed and grown that business, we have done so in the context of our longstanding commitment to consumer privacy. This commitment to consumer privacy is reflected in the way we have built and deployed our online advertising business, as described above and throughout our responses.

3. In what communities, if any, has your company engaged in such practice, how were those communities chosen, and during what time periods was such practice used in each? If such practice was effectively implemented nationwide, please say so.

This question seems to be directed at network operators and Internet service providers engaged in deep packet inspection. To reiterate, Microsoft does not engage in deep packet inspection. We tailor advertising to visitors to our website and other websites with which we partner to deliver relevant online advertising to consumers. Because the websites on which Microsoft delivers advertisements are available worldwide, our online advertising practices are effectively global and therefore nationwide.

4. How many consumers have been subject to such practice in each affected community, or nationwide?

This question seems to be directed at network operators and Internet service providers engaged in deep packet inspection. To reiterate, Microsoft does not engage in deep packet inspection. As described above, Microsoft's delivery of relevant advertising is directed to the millions of users around the world who come to our website, conduct searches on our Live.com search engine, or visit a partner site on which Microsoft serves ads.

5. Has your company conducted a legal analysis of the applicability of consumer privacy laws to such practice? If so, please explain what that analysis concluded.

Yes. Our online advertising practices are compliant with all applicable laws, and we believe we are an industry leader with respect to the privacy protections we offer consumers online. We post a prominent and clear privacy policy on every page of our website; we offer consumers robust choice before using their information to deliver relevant ads online; and we take meaningful steps to protect the security of the data we maintain.

6. How did your company notify consumers of such practice? Please provide a copy of the notification. If your company did not specifically or directly notify affected consumers, please explain why this was not done.

Microsoft is committed to being transparent about its online advertising practices. We post a link to our privacy notice on every page of our websites, including the home page.

We also were one of the first companies to develop so-called "layered" privacy notices that give clear and concise bullet-point summaries of our practices in a short notice, with links to the full privacy statement for consumers and others who are interested in more detailed information. And our privacy statement is clear about the data we collect and use for online advertising. For instance, the "top layer" of our privacy notice, contains the following bullets related to our efforts to provide users more relevant advertising:

- We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.
- We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.
- To opt-out of the display of personalized advertisements, go to the Display of Advertising section of the full privacy statement.

Our full privacy statement contains the following section:

> **Display of Advertising**
>
> Many of the Web sites and online services we offer, as well as those of our partners, are supported by advertising. Through the Microsoft Advertising Platform, we may display ads on our own sites and the sites of our advertising partners.
>
> When we display online advertisements to you, we will place a persistent cookie on your computer in order to recognize your computer each time we display an ad to you. Because we may serve advertisements on many different Web sites, we are able to compile information over time about where you, or others who are using your computer, saw and/or clicked on the advertisements we display. We use this information to make predictions about your

characteristics, interests or preferences and to display targeted advertisements that we believe may be of interest to you. We may also associate this information with your subsequent visit, purchase or other activity on participating advertisers' Web sites in order to determine the effectiveness of the advertisements.

While we may use some of the information we collect in order to personalize the ads we show you, we designed our systems to select ads based only on data that does not personally and directly identify you. For example, we may select the ads we display according to certain general interest categories or segments that we have inferred based on (a) demographic or interest data, including any you may have provided when creating an account (e.g. age, zip or postal code, gender), demographic or interest data acquired from other companies, and a general geographic location derived from your IP address, (b) the pages you view and links you click when using Microsoft's and its advertising partners' Web sites and services, and (c) the search terms you enter when using Microsoft's Internet search services, such as Live Search.

When we display personalized ads, we take a number of steps designed to protect your privacy. For example, we store page views, clicks and search terms used for ad personalization separately from your contact information or other data that directly identifies you (such as your name, e-mail address, etc.). Further, we have built in technological and process safeguards designed to prevent the unauthorized correlation of this data. We also give you the ability to opt-out of personalized ads. For more information or to use the opt-out feature, you may visit our opt-out page.

We also provide third party ad delivery through our Atlas subsidiary, and you may read the Atlas privacy statement at http://www.atlassolutions.com/privacy.aspx.

Although the majority of the online advertisements on Microsoft sites are displayed by Microsoft, we also allow third-party ad serving companies, including other ad networks, to display advertisements on our sites. These companies currently include, but are not limited to: 24/7 Real Media, Advertising.com, Bidclix, BlueStreak, Burst Media, DoubleClick, EuroClick, Eyeblaster, EyeWonder, Falk, Interpolls, Kanoodle, Mediaplex, Pointroll, TangoZebra, Yahoo! Publisher Network, and Zedo.

These companies may offer you a way to opt out of ad targeting based on their cookies. You may find more information by clicking on the company names above and following the links to the Web sites of each company. Some of these companies are members of the Network Advertising Initiative, which offers a single location to opt out of ad targeting from member companies.

Additionally, we have made available even more detailed information in our effort to be transparent about our practices. For example, we have published a white paper that describes the methods we use to "de-identify" data used for ad targeting.[2]

7. Please explain whether your company asked consumers to "opt in" to the use of such practice or allowed consumers who objected to "opt out." If your company allowed consumers who objected to opt out, how did it notify consumers of their opportunity to opt out? If your company did not specifically or directly notify affected consumers of the opportunity to opt out, please explain why this was not done.

In July 2007, Microsoft was the first major online advertising provider to announce it would give customers the opportunity to opt out of receiving targeted advertising on **all** of the web sites where Microsoft provided advertising, including both Microsoft sites and third-party partner Web sites. This opt-out option became available in the Spring of 2008. We prominently provide information and links to our opt-out mechanism in the top-layer of our privacy statement and in our full privacy statement.

Not only was Microsoft the first advertising provider to offer this type of opt-out choice to consumers, but Microsoft's opt-out choice is unique from any other offered in industry today because it is more persistent and applies across multiple computers. As background, the industry-standard approach for offering an opt-out choice is merely to place an "opt-out" cookie on their machines. While this process generally works well, it does have some inherent limitations. For example, opt-out cookies are computer-specific — if a consumer switches computers, he or she will need to specify any opt-out preferences again. Similarly, if cookies are deleted, that user's opt-out choice is no longer in effect. To address these limitations, the mechanism Microsoft offers gives consumers the option to associate their opt-out choice to their Windows Live ID. This means that even if they delete cookies on their machine, when they sign back in their opt-out choice will persist. It also means that a single choice can apply across multiple computers that they use. This will help ensure that consumers' choices are respected without requiring undue effort on their part.[3]

8. How many consumers opted out of being subject to such practice?

Consumers may opt out of receiving relevant advertising from Microsoft by following the link on the first layer of our privacy notice available at http://www.microsoft.com/info/privacy/default.mspx. Since the release of Microsoft's opt-out mechanism in the Spring of 2008, our systems indicate it has been used approximately 1800 times.[4] Additionally, consumers may choose to only place an opt-out cookie on their machine, rather than use the option of associating their choice with their Windows Live ID. From a

---

[2] *See* "Privacy Protections in Microsoft's Ad Serving System and the Process of "De-identification," available at http://www.microsoft.com/privacy.

[3] Microsoft's online advertising opt-out page is available at https://choice.live.com/advertisementchoice/Default.aspx.

[4] This may not be a perfect correlation to the number of consumers who have actually used the feature, for example a single user may deploy the opt-out solution on multiple computers, a single user may maintain multiple user accounts with Microsoft, or as a result of the issues described in our response to Question #7.

technical perspective, we are unable to estimate how many consumers utilize the cookie-only opt-out option.[5]

In addition, the Atlas advertising network, which was part of Microsoft's acquisition of aQuantive last year, maintains its own cookie-based opt-out method, which is available at http://www.atlassolutions.com/opting.aspx?cookieStatus=activeCookie. This method informs consumers of their opt-out status and allows them to opt out of receiving relevant online ads in one click. Consumers can also opt out of Atlas cookies through a link on the Network Advertising Initiative website, which is available at https://www.networkadvertising.org/managing/opt_out.asp. For the reasons stated above, we are also unable to estimate how many users have utilized this cookie-based opt-out option.

9. Did your company conduct a legal analysis of the adequacy of any opt-out notice and mechanism employed to allow consumers to effectuate this choice? If so, please explain what that analysis concluded.

Yes. As mentioned in response to Question 5, our online advertising practices, including our opt-out notice and mechanism, meet or exceed the requirements of all applicable laws. We believe the steps we have taken have encouraged other online advertising providers to improve their privacy practices online.

10. What is the status of consumer data collected as a result of such practice? Has it been destroyed or is it routinely destroyed?

Microsoft's policy is to anonymize its search log data after 18 months, which we believe is an appropriate timeframe in our circumstances to enable us to maintain and improve the security, integrity and quality of our services. We intend to continue to look for ways to reduce this timeframe while addressing security, integrity and quality concerns. In addition, unlike other companies, our anonymization method involves irreversibly removing the *entire* IP address and other cross-session identifiers, such as cookies and other machine identifiers, from search terms. Some companies remove only the last few digits of a consumer's IP address, which means that an individual search query may still be narrowed down to a small number of computers on a network. We think that such partial methods do not fully protect consumer privacy, so we have chosen an approach that renders search terms truly and irreversibly anonymous. Search and web browsing data collected in association with the aQuantive cookie is not kept for longer than 24 months and generally is not retained for longer than 13 months.

We have also designed our systems and processes in ways that minimize their privacy impact from the outset while simultaneously promoting security. We use a technical method (known as a one-way cryptographic hash) to separate records of search terms and browsing behavior from records of account

[5] From a technical perspective, the systems treat all machines with an "opt out" cookie as if the machine does not have a cookie present. As a result, we do not have a reliable way of distinguishing users who opt out of relevant advertising by using an opt-out cookie from users who actually do not have any cookie set (or who have configured their Internet browser to block all cookies).

holders' personal information, such as name, email address, and phone number, and to keep them separated in a way that prevents them from being easily recombined. We have also relied on this method to ensure that we use only data that does not personally identify individual consumers to serve ads online. As a result of this "de-identification" process, search query data and data about Web surfing behavior used for ad targeting is associated with an anonymized identifier rather than an account identifier that could be used to personally and directly identify a consumer.[6]

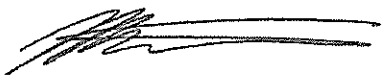
11. Is it possible for your company to correlate data regarding consumer Internet use across a variety of services or applications you offer to tailor Internet advertising? Do you do so? If not, please indicate what steps you take to make sure such correlation does not happen. If you do engage in such correlation, please provide answers to all the preceding questions with reference to such correlation. If your previous answers already do so, it is sufficient to simply cross-reference those answers.

As described in greater detail above, the data we use for ad targeting comes from several sources, including the demographic data provided by users who register for a Windows Live ID, search query data from users of Microsoft's Live Search service, and the pages viewed or links clicked when using Microsoft's and its advertising partners' Web sites and services. This data is "de-identified" so as to keep is separate from records that contain information that can directly identify a user, and it is used to infer certain general interest categories or segments that can be used to target advertisements.

* * *

Microsoft recognizes that the protection of consumer privacy is a continuous journey, not a single destination. We can and will continue to develop and implement new privacy practices and protections for consumers. We look forward to working with you to ensure consumers' privacy interests are protected as they continue to enjoy the proliferation of free services and information that online advertising supports.

Sincerely,



Michael Hintze
Associate General Counsel
Microsoft Corporation

[6] As noted above, a white paper describing Microsoft's "de-identification" process is available at http://www.microsoft.com/privacy.

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.

Microsoft®