



November 6, 2009

VIA ELECTRONIC FILING

Federal Trade Commission
Office of the Secretary, Room H-135 (Annex P)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Privacy Roundtables — Comment, Project No. P095416

Dear Secretary Clark:

Microsoft is pleased to submit these comments in response to the Commission's request for comments for its first privacy roundtable discussion. Microsoft supports the Commission's goal of exploring the privacy challenges posed by the vast array of 21st century technology and business practices involving the collection and use of consumer data. We also appreciate the Commission's ongoing efforts to work cooperatively with all stakeholders to ensure that consumers' privacy expectations are met and that the benefits of these new technologies and business models are fully realized.

Consumers are experiencing incredible benefits with an ever-evolving array of technical innovations. These include:

- Online advertising, which is considered the engine that drives the Internet economy. Online advertising has allowed thousands of websites to offer their content and services online for free to consumers. It also has created new ways for businesses to inform consumers about their products and services and enabled consumers to receive ads that they are more likely to find relevant.
- Cloud computing, which gives users the ability to combine the power and reliability of software running on their own PC or other devices with the ease and efficiency of computing delivered as a service over the Internet. Cloud computing offers tremendous opportunities, giving enterprises and consumers greater choice and flexibility while driving significant efficiency gains, lowering IT costs, and creating incentives and online platforms for innovation.
- Health IT, which enables patients to connect their health data and share it securely from provider to provider. This allows consumers to receive better information about appropriate treatments and gives providers access to more reliable data, enabling them to make better medical decisions and to develop new therapies and cures. Health IT is a critical part of important healthcare reforms leading to better quality care and lower costs.

Microsoft has a deep and long-standing commitment to protecting consumer privacy across technologies and business models. We were one of the first companies to appoint a chief privacy officer, an action we took over a decade ago, and we have consistently designed our products and services in a way that protects consumer privacy. For example, we adopted meaningful privacy practices around search and online advertising early on and, in 2007, released “Privacy Principles for Live Search and Online Ad Targeting” that articulated industry leading practices for these evolving business models. In addition, in an effort to share our experience with designing privacy protections onto software and online services and promote industry-wide best practices in software design and development, we released “Privacy Guidelines for Developing Software Products and Services” in 2006, and updated those guidelines in 2008 to take into account evolving business practices.

In the end, Microsoft has adopted and advanced strong privacy protections because we recognize that consumers will only be comfortable taking advantage of the benefits of new technologies if they trust that they will have control over the use of their information and know that it will be protected.

Promoting Trust Through Transparency, Control and Security

To foster consumer trust, Microsoft believes companies that collect and use data, regardless of the technology or business model, should adhere to the following three principles: transparency, control and security. We briefly describe these three principles below and have attached supplemental documents on online advertising, cloud computing, and health IT that provide more detailed information about the application of the three principles in these contexts.

1. **Transparency:** Transparency requires entities to be clear about their data collection, use, and disclosure practices. Without transparency, consumers are unable to evaluate an entity’s services, to compare the privacy practices of different entities to determine which products and services they should use, or to exercise the privacy controls that may be available to them. Transparency also helps ensure that when consumers are dealing with a company that has adopted reasonable privacy practices, they do not needlessly worry about unfounded privacy concerns, which could prevent them from participating in the online ecosystem or taking advantage of new technologies.

2. **Control:** Control requires entities to give consumers choices about the use of their data based on the level of privacy risks involved. For example, consumers should have a choice about whether information about their online activities is used to create behavioral profiles for targeted advertising. In the context of cloud computing, consumers and enterprises should be given flexibility and choice about the data, software, and applications that are kept locally and when computing delivered as a service over the Internet is preferred. And patients should have control over where their health data is, who is looking at it, and for what purpose.

3. **Security:** Security requires entities to take reasonable steps to protect user data against outside threats and from unwanted disclosures. With respect to online behavioral

advertising, data that directly identifies individual consumers, such as name and e-mail address, should not be stored in association with search terms or data about Web surfing behavior used to deliver ads online. In the context of cloud computing, strong security practices, meaningful policies, and effective controls must be adopted to help protect the datacenters themselves and the information stored therein. Where highly sensitive data, such as health records, are involved, strong measures to protect against the unauthorized access or misuse of such data — including technologies that verify patients’ identities, monitor access to health records, and identify anomalies in services requested — are important.

Microsoft believes that the Commission’s privacy initiatives should be shaped by these principles of transparency, control, and security. We applaud the Commission for using these principles as the framework for self-regulatory principles governing online behavioral advertising earlier this year.

Supporting Comprehensive Federal Privacy Legislation

Microsoft believes that the principles of transparency, choice and security also serve as an effective framework for comprehensive federal privacy legislation. We have long viewed federal privacy legislation as an important component of effective privacy protection. Federal privacy legislation also will help address the existing patchwork of federal and state privacy laws in the U.S., which has led to an overlapping, inconsistent and incomplete set of obligations for businesses and uncertainty for consumers.

Under a federal privacy legislative framework, general notice, choice, and security obligations should apply to all entities that use consumer information for any purpose. Additional obligations within these contexts should depend on the different risks to consumers inherent in different types of information and the entity’s intended use or disclosure of such information. Microsoft believes that federal privacy obligations should apply to both online *and* offline data practices to ensure consumers’ privacy is protected regardless of how information is collected or the type of organization using it.

Acknowledging and Supporting the Role of Self-Regulation

While a comprehensive federal privacy law should establish a baseline common set of privacy and security requirements, legislation is not a complete solution. Rapidly changing business models and innovations may merit a more flexible and multifaceted approach. In many cases legislation can be even more effective if it can work in conjunction with industry self-regulation and best practices, technology solutions, and consumer education. In the end, self-regulation can and should complement baseline federal privacy protections by providing targeted obligations based on transparency, control, and security that can quickly evolve to address advancements in technologies and developments in business models.

In the context of online advertising, for example, several industry groups came together over the summer to adopt self-regulatory principles based on the principle of transparency and choice to address new and rapidly evolving business models and practices.

Microsoft has supported this and other self-regulatory efforts that protect consumer privacy while accommodating important differences inherent in different business practices. This approach can provide an effective mechanism for ensuring the privacy of consumers while allowing for an evolving marketplace and to help foster continued robust online content.

Defining Obligations Based on the Use of Information

In applying the principles of transparency, control, and security, the Commission, Congress and industry self-regulatory principles should focus on an entity's intended use of consumer data and the type of information at issue (e.g., IP address vs. sensitive identifiable health information). Microsoft believes the use of consumer data, rather than its collection, serves as a better starting point for defining privacy obligations. This "use-and-obligations" model requires all organizations to be transparent, offer and honor appropriate choice, ensure that risks to consumers related to the use of their information are assessed and managed, and secure the information they maintain.

This model in no way lessens the requirement that information be collected in a fair and lawful manner. Rather, it provides a governance approach that is more manageable for business and more effective for consumers by imposing higher obligations on data practices that pose greater privacy risks. As a result, this approach avoids creating impediments to legitimate and necessary collections of consumer information. In addition, the use-and-obligations model takes into account all the intended uses of information, and therefore avoids the need to draw distinctions between broad notions of "primary" and "secondary" uses of data. As a result, an entity's obligations are more clearly defined and consumers are better informed of their rights with respect to the use and disclosure of their information.

Addressing Global Considerations

In the end, protecting consumer privacy requires a multi-faceted approach based on meaningful legal and regulatory frameworks, industry self-regulation, consumer education, and technology tools. It also requires collaboration between the public and private sectors across all of these fronts, both in the United States and abroad.

Cloud computing presents a good example of the need for governments around the world to work with industry to adopt harmonized and coordinated rules around consumer privacy. With the growth in online computing, increasing amounts of user data are being processed and transferred across national borders. However, divergent claims to jurisdiction over user content and data held by providers of cloud computing services, and conflicting national rules on data privacy, data retention, and law enforcement access to user data, among other issues, make it extremely difficult for providers to manage their legal obligations and give consumers adequate notice and assurance of their data protection practices.

Industry has been working hard to address these problems. For example, online computing providers are expending considerable resources to ensure that their physical operations and corporate structure minimize the problems posed by conflicting legal rules —

often at the expense of the efficiencies and other benefits cloud computing can provide. But these efforts cannot entirely solve the problem; for both business and technical reasons, it simply is impractical to locate servers in every jurisdiction or to strictly segregate data in multiple locations based on the presumed location of users.

Therefore, it is essential that governments around the world work with industry to adopt harmonized, coordinated rules for access to, and the protection of, online user data. Given the importance of the Internet to U.S. competitiveness and economic growth, the U.S. federal government has a unique interest in assuming leadership on these issues so that the many benefits of cloud computing may be realized. We look forward to engaging with the Commission and other government leaders on this important issue.

* * *

Microsoft is prepared to work collaboratively on all fronts to protect consumer privacy and appreciates the opportunity to submit these comments in connection with the Commission's roundtable discussions. If you have any questions about our comments, please do not hesitate to let me know.

Respectfully submitted,

Michael D. Hintze
Associate General Counsel
Microsoft Corporation

Attachments

- Statement of Michael D. Hintze, Associate General Counsel, Microsoft Corporation, Before the Committee on Commerce, Science & Transportation, United States Senate, Privacy Implications of Online Advertising (July 9, 2008)
- Privacy in the Cloud Computing Era: A Microsoft Perspective (Nov. 2009)
- Written Testimony of Michael Stokes, Principal Program Manager, Microsoft Corporation's Health Solutions Group, Before the Senate Judiciary Committee, Hearing on Health IT: Protecting Americans' Privacy in the Digital Age (Jan. 27, 2009)

**Attachment A:
Statement of Michael D. Hintze Before the
Senate Committee on Commerce, Science
& Transportation**

Statement of Michael D. Hintze
Associate General Counsel
Microsoft Corporation

Before the
Committee on Commerce, Science & Transportation
United States Senate

“Privacy Implications of Online Advertising”

July 9, 2008

Chairman Inouye, Ranking Member Stevens, and honorable Members of the Committee, my name is Michael Hintze, and I am an Associate General Counsel of Microsoft Corporation. Thank you for the opportunity to share Microsoft's views on the important privacy issues presented by advertising on the Internet. We appreciate the initiative that this Committee has taken in holding this hearing, and we are committed to working collaboratively with you, the Federal Trade Commission, consumer groups, and other stakeholders to protect consumers' privacy interests online.

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. It supports the ability of websites to offer their content and services online; it has created new opportunities for businesses to inform consumers about their products and services; and it allows consumers to receive ads they are more likely to find relevant. Simply stated, the Internet would not be the diverse and useful medium it has become without online advertising.

At the same time, online advertising is unique because it can be tailored automatically to a computer user's online activities and interests. An online ad can be served based on the website a user is visiting, the searches a user is conducting, or a user's past Internet browsing behavior, among other things. In each instance, serving the online advertisement involves the collection of information about consumers' Internet interactions. And this data collection has implications for consumer privacy.

The objective we face is to maintain the growth of online advertising while protecting consumer privacy. This is a commitment Microsoft embraces. We recognize

that consumers have high expectations about how we and other Internet companies collect, use, and store their information. Consumers must *trust* that their privacy will be protected. If the Internet industry fails to meet that standard, consumers will make less use of online technologies, which will hurt them and industry alike.

It also could hurt the U.S. economy. E-commerce sales reached \$136.4 billion in 2007, an increase of 19% from 2006, according to the U.S. Census Bureau.¹ In comparison, total retail sales in 2007 increased only 4% from 2006. 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 robust privacy practices that build trust with consumers.

Microsoft has a deep and long-standing commitment to consumer privacy. 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 a robust set of internal policies and standards that guide how we do business and how we design our products and services in a way that respects and protects user privacy.² And we have made significant investments in privacy in terms of training and by building our privacy standards into our product development and other business processes.

¹ U.S. Census Bureau, *Quarterly Retail E-Commerce Sales: 4th Quarter 2007*, Feb. 15, 2008, available at <http://www.census.gov/mrts/www/data/html/07Q4.html>.

² Some of these standards are set forth in Microsoft's Privacy Principles for Live Search and Online Ad Targeting, attached as Appendix 1. This document is also available at <http://www.microsoft.com/privacy>. Additionally, Microsoft's Privacy Guidelines for Developing Software Products and Services, which are based on our internal privacy standards, are available at <http://www.microsoft.com/privacy>.

In general, three key principles have guided our approach to privacy issues:

- *Transparency.* We believe consumers should be able to easily understand what information will be collected about them and when. They also should know how such information will be used and whether it will be combined with other information collected from or about them.
- *Control.* We believe consumers should be able to control whether their personal information is made available to others and should have a choice about whether information about their online activities is used to create profiles for targeted advertising.
- *Security.* Consumers and their information should be protected against outside threats and from unwanted disclosure. Data that directly identifies individual consumers, such as name and email address, should not be stored in direct association with search terms or data about Web surfing behavior used to deliver ads online. And strict data retention policies should apply to search data.

Today, I will discuss why we believe these principles are important, how we have put each of these principles into action, and how they underlie Microsoft's approach to privacy in online advertising. But first I would like to provide an overview of how online advertising works, the role that consumer data plays in serving online ads, and the online advertising market.

I. ONLINE ADVERTISING AND THE ROLE OF USER DATA

Consumers today are able to access a wealth of information and a growing array of services online for free. Websites can offer this content and these services for free because of the income they receive from advertising.³ Just as newspapers and TV news programs rely on traditional advertising, online news sites and other commercial websites rely on online advertising for their economic survival. Online advertising is particularly critical for

³ It has become a standard approach to the online economy that there is a value exchange in which companies provide online content and services to consumers without charging a fee and, in return, consumers see advertisements that may be targeted.

the thousands of smaller websites that do not publish through offline channels and thus depend entirely on the revenue they receive from selling space on their websites to serve ads online. It is also critical for smaller businesses that serve niche markets (e.g., out-of-print books on European history) who rely on online advertising to reach those niche audiences cost-effectively; indeed, many of these businesses could not survive without it.

The importance of online advertising is evident from its growing share of the overall advertising market. It accounted for \$21 billion of the market in 2007 and is expected to grow to \$50 billion in the next three years.⁴ In the United States, online advertising spending already exceeds spending for advertising through radio, magazines, and cable television.⁵

One reason for this rapid growth is the ability to target online ads to Internet users. Newspaper, magazine, and television advertisements can, of course, be targeted based on the broad demographics of readers or viewers. But the Internet is interactive, and this interaction yields a wealth of data about users' activities and preferences. Each search, click, and other user action reveals valuable information about that user's likely interests. The more information an entity collects, the greater that entity's ability to serve an advertisement that is targeted to the user's interests. This targeting benefits users, not only because it enables the free services and content they enjoy, but also because the ads

⁴ See Interactive Advertising Bureau, *IAB Internet Advertising Revenue Report*, 7, May 2008, available at http://www.iab.net/media/file/IAB_PwC_2007_full_year.pdf; Yankee Group, *Yankee Group Forecasts US Online Advertising Market to Reach \$50 Billion By 2011*, Jan. 18, 2008, available at <http://www.yankeegroup.com/pressReleaseDetail.do?actionType=getDetailPressRelease&ID=1805>.

⁵ See Brian Morrissey, *IAB: Web Ad Spend Tops Cable, Radio*, ADWEEK, May 15, 2008, available at http://www.adweek.com/aw/content_display/news/digital/e3ibcf6d45fc7a036dff28457a85c838ff1.

they see are more likely to be relevant. And it benefits advertisers because users are more likely to respond to their ads.⁶

There are a variety of ways in which data can be collected about users to serve targeted ads on the Internet. Users reveal information about what they are looking for when they search online, and ads can be targeted to their search queries.⁷ Advertising networks enter into agreements with websites that allow them to display ads; to deliver and target those ads, data is gathered about the pages users view and the links users click on within those sites.⁸ And new business models are emerging where data about users' online activities can be collected through a user's Internet service provider, and ads can be served based on that information. In general, most data collection happens in connection with the display of ads. This means the entity that serves the most ads (search and/or non-search ads) will also collect the most data about users.

⁶ It is for this reason advertisers are willing to pay more for targeted ads. For example, although Merrill Lynch has reported that the average cost per 1000 impressions ("CPM") is \$2.50, entities engaged in behavioral targeting have reported average CPMs as high as \$10. See Brian Morrissey, *Aim High: Ad Targeting Moves to the Next Level*, ADWEEK, Jan. 21, 2008, available at http://www.adweek.com/aw/magazine/article_display.jsp?vnu_content_id=1003695822. Data also shows that 57% of 867 search engine advertisers and search engine marketing agencies polled "were willing to spend more on demographic targeting, such as age and gender." Search Engine Marketing Professional Organization, *Online Advertisers Are Bullish on Behavioral Targeting*, May 15, 2008, available at <http://www.sempo.org/news/releases/05-15-08>.

⁷ Search ads are selected based on the search term entered by a user and sometimes on data that has been collected about the user, such as the user's history of prior searches. Search ads generally appear either at the top of the search results or along the right-hand side of the page. They often are displayed as text, but they may include graphics as well. Advertisers bid against each other for the right to have their ads appear when a specific search term is entered (known as a "keyword").

⁸ These non-search ads are what users see when they visit virtually any site on the Internet other than a search engine site. They can be based on the content of the page the user is viewing (typically referred to as "contextual" ads) or on a profile of a user's activities that has been collected over time (referred to as "behavioral" ads). But in either case, the company serving the ad would log the pages users view – typically in association with a cookie ID from the user's computer and/or an IP address.

II. THE ONLINE ADVERTISING ENVIRONMENT

The online advertising ecosystem has undergone significant changes in the past few years. There continue to be millions of websites that display online ads and thousands of advertisers who use online advertising. However, there is a relatively small number of so-called advertising networks, or “middlemen,” to bring advertisers and websites together to buy and sell online ad space. And the number of companies playing this intermediary role has decreased significantly in recent months as a result of consolidation in the industry.⁹

This market consolidation impacts the privacy issues we are discussing today in several ways. First, it is important to recognize that in the past, advertising networks typically did not have direct relationships with consumers. Today, however, the major ad networks are owned by entities — such as Microsoft, Google, and Yahoo! — that provide a wide array of Web-based services and, therefore, often have direct relationships with consumers. This increases the potential that data collected through online advertising will be combined with personally identifiable information. While Microsoft has designed its online advertising system to address this concern,¹⁰ no ad network is required to do so.

Further, as noted above, there is a direct connection between the market share of an advertising network or an online search provider and the amount of data collected about a user’s online activity. For example, the larger the share of search ads a company delivers, the larger number of users’ online search queries it collects and stores. Similarly, the larger

⁹ Three examples of this are Microsoft’s acquisition of aQuantive, Yahoo!’s acquisition of RightMedia and Google’s acquisition of DoubleClick. For more information about the key players in the advertising market and the impact of consolidation in the market, see the testimony of Microsoft General Counsel Brad Smith before the Senate Judiciary Committee, *available at* <http://www.microsoft.com/presspass/exec/bradsmith/09-27googledoubleclick.msp>.

¹⁰ See section III.C below.

the share of non-search ads an advertising network delivers across the Web, the larger number of users' page views it collects and stores, and the more complete picture of individuals' online surfing behavior it is able to amass. Today, Google AdWords is the leading seller of search advertising.¹¹ Google also has the leading non-search ad network, AdSense. Google recently expanded its reach into non-search by acquiring DoubleClick.¹² By comparison, Microsoft is a relatively small player in search ads, and its reach in non-search advertising is also smaller than Google's.¹³ Google's growing dominance in serving online ads means it has access to and collects an unparalleled amount of data about people's online behavior.¹⁴

¹¹ Based on comScore's Core Search Report, in May of this year, 62% of searches were performed in the U.S. on Google, amounting to roughly 6.7 billion searches. comScore, *comScore Releases May 2008 U.S. Search Engine Rankings*, June 19, 2008, available at <http://www.comscore.com/press/release.asp?press=2275>. Google also has strategic agreements with AOL and Ask that allow Google to serve ads to those companies' search engine sites. Adding AOL's (4.5%) and Ask.com's (4.5%) share of the search queries, Google's share rises to 71%. *See id.*

¹² Following its acquisition of DoubleClick, Google now serves in the range of 70% of all non-search advertisements. *See, e.g., Lots of Reach in Ad . . .*, April 1, 2008, available at <http://battellemedia.com/archives/004356.php>.

¹³ Microsoft's Live Search has approximately 8.5% of Core Search queries in the United States. comScore, *comScore Releases May 2008 U.S. Search Engine Rankings*, June 19, 2008, available at <http://www.comscore.com/press/release.asp?press=2275>.

¹⁴ Concerns have been raised about this dominance as well as the privacy protections surrounding the enormous amount of information about users' online behavior that this dominance enables. *See, e.g., Electronic Privacy Information Center, Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief*, June 6, 2007, available at http://epic.org/privacy/ftc/google/supp_060607.pdf ("The combination of Google (the world's largest Internet search engine) with DoubleClick (the world's largest Internet advertising technology firm) would allow the combined company to become the gatekeeper for Internet content. . . . The detailed profiling of Internet users raises profound issues that concern the right of privacy. . . ."); *see also*, Jaikumar Vijayan, *Google Asked to Add Home Page Link to Privacy Policies*, COMPUTERWORLD, June 3, 2008, available at <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9092838>; Privacy International, *A Race to the Bottom: Privacy Ranking of Internet Service Companies*, Sept. 6, 2007, available at <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-553961> (We "witnessed an attitude to privacy within Google that at its most blatant is hostile, and at its most benign is ambivalent.").

There also is a critical relationship between competition and privacy that must not be overlooked in this discussion. Competition ensures companies have an incentive to compete on the basis of the privacy protections they offer. On the other hand, a dominant player who is insulated from competitive pressure has little reason to heed consumer demand for stronger privacy protections and faces no significant competitive pressure from other firms offering superior privacy practices. Indeed, if a dominant player could generate additional profits by diluting its privacy practices, there is a significant risk it may do so. This could bring about a “race to the bottom” on privacy as other companies weaken their privacy practices in an effort to catch up to the market leader.

Yahoo! and Google’s recently announced agreement raises important questions in this regard. Under the agreement, Yahoo! will outsource to Google the delivery of ads appearing alongside Yahoo!’s search engine results.¹⁵ This has the potential to give Google, the market leader, further control over the sites and services where ads are served, enabling Google to collect even more data about computer users and potentially to combine that data with the personal information it has on those users.¹⁶ It also will reduce competition in the search advertising market, and thereby weaken Google’s incentives to compete on the quality of its privacy practices. Both of these outcomes have implications for consumer privacy.¹⁷

¹⁵ See http://www.google.com/intl/en/press/pressrel/20080612_yahoo.html.

¹⁶ With Google’s 71% search query share in the U.S. based on its relationship with AOL and Ask.com (see *supra* fn. 11), in combination with Yahoo’s 20.6% share of the core search query market, Google will be able to gather information on up to 92% of online searches. See comScore, *comScore Releases May 2008 U.S. Search Engine Rankings*, June 19, 2008, available at <http://www.comscore.com/press/release.asp?press=2275>.

¹⁷ See Jeff Chester, *A Yahoo! & Google Deal Is Anti-Competitive, Raises Privacy Concerns*, May 22, 2008, available at <http://www.democraticmedia.org/jcblog/?p=596>.

III. MICROSOFT'S COMMITMENT TO PRIVACY IN ONLINE ADVERTISING

Microsoft recognizes the role that data plays in online advertising and the corresponding importance of protecting consumer privacy. To guide our approach to data collection for online advertising, we released Microsoft's Privacy Principles for Live Search and Online Ad Targeting last July.¹⁸ We are deeply committed to these principles, which focus on bringing the benefits of transparency, control and security to the protection of consumers' data and privacy online.

A. Transparency

I want to first touch upon the importance of transparency. Transparency is significant because it provides consumers with an informed understanding of a company's data collection practices, of how their data might be used, and the privacy controls available to users. Without transparency, consumers are unable to evaluate a company's services, to compare the privacy practices of different entities to determine which online products and services they should use, or to exercise the privacy controls that may be available to them. Transparency also helps ensure that when consumers are dealing with a company that has adopted responsible privacy practices, they do not needlessly worry about unfounded privacy concerns, which could prevent them from taking advantage of new technologies.

Transparency is also essential to ensure accountability. Regulators, advocates, journalists and others have an important role in helping to ensure that appropriate privacy practices are being followed. But they can only examine, evaluate and compare practices

¹⁸ See Appendix 1. Microsoft's Privacy Principles for Live Search and Online Ad Targeting are also available at <http://www.microsoft.com/privacy>.

across the industry if companies are transparent about the data they collect and how they use and protect it.

Transparency is especially important with respect to online advertising. This is because consumers may not understand the types of information that entities collect or log in providing advertisements online. For example, many consumers may not realize that information about the pages they are viewing, the searches they are conducting, or the services they are using may be collected and used to deliver online ads.

For this reason, Microsoft believes that *any* entity that collects or logs *any* information about an individual or computer for the purpose of delivering advertisements online should provide clear notice about its advertising practices. This means posting a conspicuous link on the home page of its website to a privacy statement that sets forth its data collection and use practices related to online advertising. Consumers should not be required to search for a privacy notice; it should be readily available when they visit a website. This obligation should apply to entities that act as ad networks, as well as to websites on which ads appear — whether they display ads on their own or rely on third parties to deliver online advertising.

In addition to being easy to find, the privacy notice must be easy to understand. While many websites have publicly posted a privacy notice, this alone is not enough. Too often, the posted privacy notice is complex, ambiguous and/or full of legalese. These notices make privacy practices more opaque, not more transparent. Instead, short and simple highlights are essential if consumers are to easily understand a company's

information practices. It helps avoid the problem of information overload, while enabling consumer awareness.

Finally, to ensure that the consumer can be fully informed, the privacy notice should also describe the website's data collection and use activities in detail. This includes, at a minimum, descriptions of the types of information collected for online advertising; whether this information will be combined with other information collected from or about consumers; and the ways in which such information may be used, including whether any non-aggregate information may be shared with a third party.

Microsoft has embraced these obligations. 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. Further, we have released more detailed information about our practices, such as a white paper that describes the methods we use to "de-identify" data used for ad targeting.¹⁹ To illustrate our efforts to be transparent about our practices, we have included in Appendix 2 screen shots of the privacy link available on the home page of our Windows Live search service and of our layered privacy notice, including both the short notice and our full online privacy statement.

¹⁹ See section III.C below.

B. Control

The second core principle Microsoft looks to in protecting our customers' privacy is user control. Consumers should have a choice about how information about their online activities is used, especially when that information can be aggregated across multiple websites or combined with personal information. Microsoft has made consumer control a key component of our practices online.

As an example, Microsoft has recently deployed a robust method to enable users to opt out of behavioral ad targeting. As background, most industry players that offer consumers a choice about having information about their online activities used to serve behaviorally targeted ads do so by offering consumers the ability to place an "opt-out" cookie on their machines. In general, this process works well, but 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. Further, if cookies are deleted from the user's PC, that user's opt-out choice is no longer in effect. To address these limitations, Microsoft now gives consumers the option to tie 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 selection 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.²⁰

Microsoft also has committed to respecting consumers' opt-out choice on all sites where it engages in behavioral advertising. This means that consumers are offered a

²⁰ Microsoft's personalized advertising opt-out page is available at <https://choice.live.com/advertisementchoice/Default.aspx>.

choice about receiving behaviorally targeted ads across both third-party websites on which Microsoft delivers behaviorally targeted ads, as well as Microsoft's own websites. This is important because consumers reasonably expect that the opt-out choice offered by a company would apply on all websites where that company engages in behavioral advertising practices. This is another example of where we have committed to going beyond standard industry practice to better protect the interests of consumers.

We also recognize it is appropriate that the level of consumer control may vary depending on the data that will be used to serve an online ad. For example, many consumers have serious reservations about the receipt of targeted advertising based on the use of certain categories of personally identifiable information, particularly those that may be considered especially sensitive. Thus, we have proposed that companies should obtain additional levels of consent for the use of such information for behavioral advertising — including affirmative opt-in consent for the use of sensitive personally identifiable information.²¹

C. Security

The third principle we look to in protecting consumers' privacy is that strong, simple, and effective security is needed to strengthen consumers' trust in our products, the Internet, and all information technologies. Security has been fundamental at Microsoft for many years as part of our Trustworthy Computing initiative. And it plays a key role with respect to our online advertising practices.

²¹ See, for example, Microsoft's comments to the Federal Trade Commission's proposed self-regulatory framework for online advertising, included as Appendix 4 and available at <http://www.ftc.gov/os/comments/behavioraladprinciples/080411microsoft.pdf>.

We have taken a broad approach to protecting the security of computer users with respect to serving ads online. This approach includes implementing technological and procedural protections to help guard the information we maintain. We also have taken steps to educate 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 security issues.

In addition, we have designed our systems and processes in ways that minimize their privacy impact from the outset while simultaneously promoting security. For example, we use a technical method (known as a one-way cryptographic hash) to separate search terms from 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. 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.²²

Finally, we have implemented strict retention policies with respect to search query data. Our policy is to anonymize all such 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

²² A white paper describing Microsoft's "de-identification" process is attached to these comments as Appendix 3. It is also available at <http://www.microsoft.com/privacy>.

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.

IV. MICROSOFT'S SUPPORT FOR SELF-REGULATION AND PRIVACY LEGISLATION

Microsoft believes that these core principles of transparency, control, and security are critical to protecting consumers' privacy interests online. These principles form the basis for our support of robust self-regulation in the online advertising market and for baseline privacy legislation.

We have been an active participant in self-regulatory efforts. Microsoft has been engaging with the Network Advertising Initiative ("NAI"), a cooperative of online marketing and advertising companies that addresses important privacy and consumer protection issues in emerging media.²³ The NAI is currently in the process of revising its guidelines to address changes in the online advertising industry. The NAI's efforts have been critical to understanding the privacy issues associated with online advertising, and we will continue to work with them as they finalize their draft proposal.

²³ Atlas, which was part of Microsoft's recent acquisition of aQuantive, was a founding member of NAI.

We also filed comments responding to the Federal Trade Commission's request for input on a proposed self-regulatory framework for online advertising. In our comments, we explained the need for a broad self-regulatory approach since all online advertising activities have potential privacy implications and some may be contrary to consumers' expectations. To this end, we proposed a tiered approach to self regulation that is appropriately tailored to account for the types of information being collected and how that information will be used. It would set a baseline set of privacy protections applicable to all online advertising activity and would establish additional obligations for those companies that engage in practices that raise additional privacy concerns. We are attaching a copy of our comments to the FTC for your convenience.²⁴

In addition to supporting self-regulatory efforts, we have long advocated for legislation as a component of effective privacy protections. We were one of the first companies to actively call for comprehensive federal privacy legislation.²⁵ More recently, we have supported balanced and well-crafted state legislation on privacy in online advertising that would follow the general structure proposed in our FTC comments.²⁶ And we would be glad to work with the Committee on similar national privacy standards that

²⁴ See Appendix 4. Our comments are also available at <http://www.ftc.gov/os/comments/behavioraladprinciples/080411microsoft.pdf>.

²⁵ See <http://www.microsoft.com/presspass/download/features/2005/PrivacyLegislationCallWP.doc>.

²⁶ A. 9275-C, 2007-2008 Reg. Sess. (N.Y. 2008), *available at* <http://assembly.state.ny.us/leg/?bn=A09275&sh=t> (imposing minimum notice and choice obligations on certain website publishers and advertising networks); S. 6441-B, 2007-2008 Reg. Sess. (N.Y. 2008), *available at* <http://assembly.state.ny.us/leg/?bn=S06441&sh=t> (imposing baseline notice, choice, security, and consumer access obligations on certain third-party advertising networks); H.B. 5765, 2008 Gen. Assem., Feb. Sess. (Conn. 2008), *available at* <http://www.cga.ct.gov/2008/FC/2008HB-05765-R000148-FC.htm> (imposing minimum notice, choice, security, and use limitations on third-party advertising networks).

would protect both privacy and opportunities for innovation in the online advertising industry.

Our support of self regulation in the online advertising market and prudent privacy legislation is only a part of our comprehensive approach to protecting consumer privacy. We will continue to support consumer education efforts to inform users of how to best protect themselves and their information online. And we will persist in our efforts to develop technology tools that promote the principles of transparency, control, and security. In short, we are prepared to work collaboratively on all fronts to maintain the growth of online advertising while fostering consumer trust online.

V. CONCLUSION

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 to bring the benefits of transparency, choice, and security to consumers. Thank you for giving us the opportunity to testify today. 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.

Appendix 1: Microsoft's Privacy Principles for Live
Search and Online Ad Targeting

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:

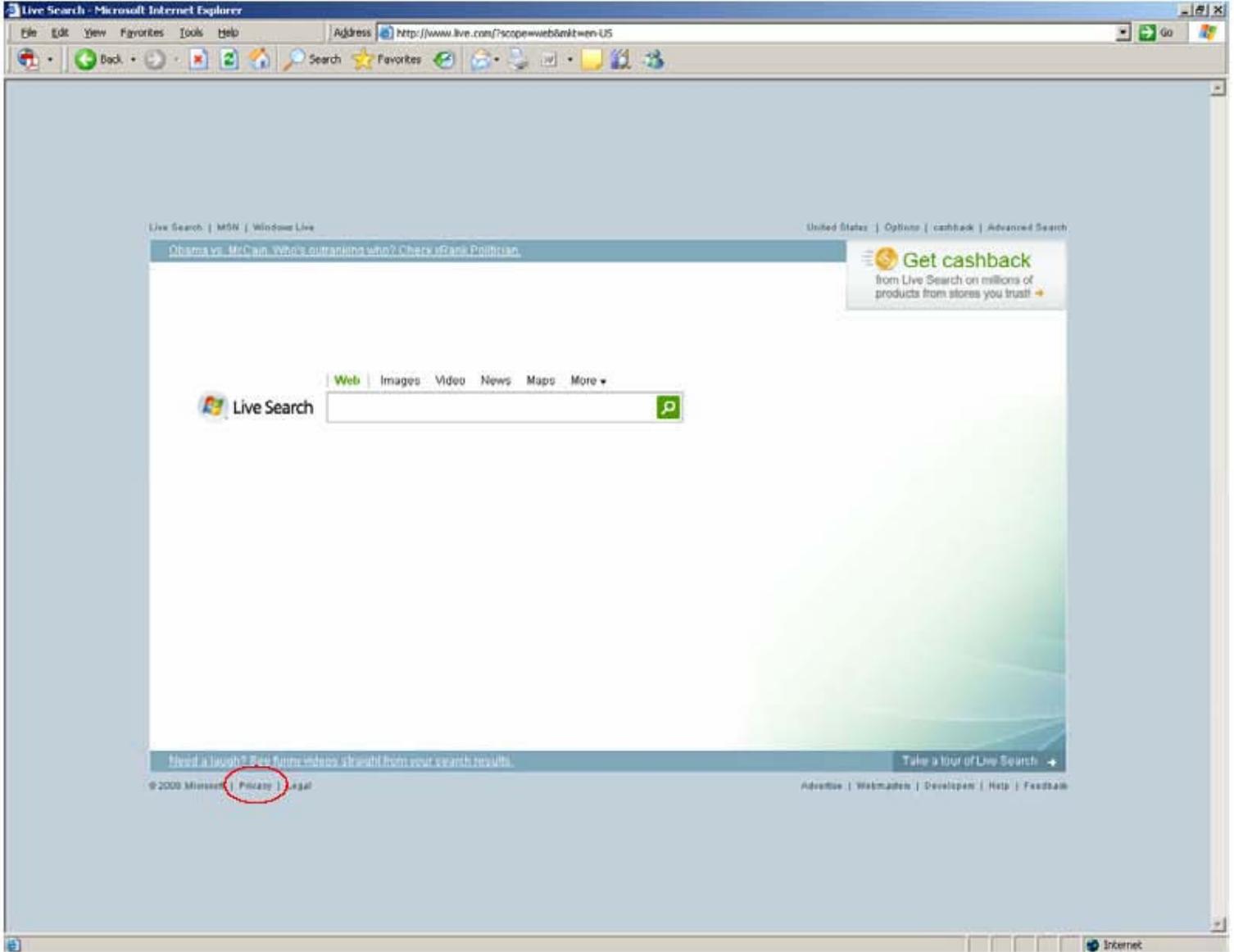
- We will store our Live Search service search terms separately from account information that personally and directly identifies the user, such as name, email address, or phone numbers (“individually identifying account information”). We will maintain and continually improve protections to prevent unauthorized 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.

Appendix 2: Microsoft's Privacy Notice



Microsoft Online Privacy Notice Highlights - Microsoft Internet Explorer

File Edit View Favorites Tools Help Address http://www.microsoft.com/info/privacy/default.aspx Go

Back Search Favorites SnagIt

Click Here to Install Silverlight United States Change All Microsoft Sites

Microsoft

Microsoft Online Privacy Notice Highlights

(last updated May 2008)



Scope

This notice provides highlights of the full [Microsoft Online Privacy Statement](#). This notice and the full privacy statement apply to those Microsoft Web sites and services that display or link to this notice.

Personal Information

[Additional Details](#)

- When you register for certain Microsoft services, we will ask you to provide personal information.
- The information we collect may be combined with information obtained from other Microsoft services and other companies.
- We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.

Uses of Information

[Additional Details](#)

- We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.
- We use your information to inform you of other products or services offered by Microsoft and its affiliates, and to send you relevant survey invitations related to Microsoft services.
- We do not sell, rent, or lease our customer lists to third parties. In order to help provide our services, we occasionally provide information to other companies that work on our behalf.

How to Contact Us

For more information about our privacy practices, go to the full [Microsoft Online Privacy Statement](#). Or write us using our [Web form](#). If you have a technical or general support question, please visit <http://support.microsoft.com> to learn more about Microsoft Support offerings.

[Top of page](#)

Your Choices

[Additional Details](#)

- You can stop the delivery of promotional e-mail from a Microsoft site or service by following the instructions in the e-mail you receive.
- To make proactive choices about how we communicate with you by e-mail, telephone, and postal mail, follow the instructions listed in the [Communication Preferences](#) of the full privacy statement.
- To opt-out of the display of personalized advertisements, go to the [Display of Advertising](#) section of the full privacy statement.
- To view and edit your personal information, go to the [access section](#) of the full privacy statement.

Important Information

- The full [Microsoft Online Privacy Statement](#) contains links to supplementary information about specific Microsoft sites or services.
- The sign in credentials (e-mail address and password) used to sign in to most Microsoft sites and services are part of the [Windows Live ID](#).
- For more information on how to help protect your personal computer, your personal information and your family online, visit our [online safety resources](#).
- Microsoft is a member of the [TRUSTe](#) privacy seal program.

© 2008 Microsoft Corporation. All rights reserved. [Contact Us](#) | [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

Start | Internet | Inbox - Microsoft Outlook | 2 Microsoft Office | Appendices 2 (rectan) | 2 Internet Explorer | 5:47 PM

[Click Here to Install Silverlight](#)[United States](#) | [Change](#) | [All Microsoft Sites](#)

Search Microsoft.com for:

Go

Microsoft Online Privacy Statement

(last updated May 2008)

[view the privacy statement highlights](#)

On This Page

- ↓ [Collection of Your Personal Information](#)
- ↓ [Use of Your Personal Information](#)
- ↓ [Sharing of Your Personal Information](#)
- ↓ [Accessing Your Personal Information](#)
- ↓ [Communication Preferences](#)
- ↓ [Display of Advertising](#)
- ↓ [Security of Your Personal Information](#)
- ↓ [Collection and Use of Children's Personal Information](#)
- ↓ [Use of Cookies](#)
- ↓ [Use of Web Beacons](#)
- ↓ [Controlling Unsolicited E-mail \("Spam"\)](#)
- ↓ [TRUSTe Certification](#)
- ↓ [Enforcement of This Privacy Statement](#)
- ↓ [Changes to This Privacy Statement](#)
- ↓ [Contacting Us](#)

TRUSTe**TO VERIFY**

Microsoft is committed to protecting your privacy. Please read the Microsoft Online Privacy Statement below and also any supplemental information listed to the right for additional details about particular Microsoft sites and services that you may use.

This Microsoft Online Privacy Statement applies to data collected by Microsoft through the majority of its Web sites and services, as well as its offline product support services. It does not apply to those Microsoft sites, services and products that do not display or link to this statement or that have their own privacy statements. Some products and services mentioned in this statement may not be available in all markets at this time.

Collection of Your Personal Information

At some Microsoft sites, we ask you to provide personal information, such as your e-mail address, name, home or work address, or telephone number. We may also collect demographic information, such as your ZIP code, age, gender, preferences, interests and favorites. If you choose to make a purchase or sign up for a paid subscription service, we will ask for additional information, such as your credit card number and billing address, which is used to create a Microsoft billing account.

In order to access some Microsoft services, you will be asked to sign in with an e-mail address and password, which we refer to as your [Windows Live ID or Microsoft Passport Network](#) credentials. You can use the same credentials to sign in to many different Microsoft sites and services, as well as those of select Microsoft partners.

Supplemental Privacy Information

- [CRM Online](#)
- [Messenger](#)
- [MSN](#)
- [Office Live](#)
- [Office Online](#)
- [Search and Maps](#)
- [Support Services](#)
- [Windows Live](#)
- [Windows Live ID / Passport](#)
- [Windows Marketplace](#)
- [Windows Live OneCare](#)
- [WindowsMedia.com](#)
- [Xbox LIVE, Games for Windows LIVE and Xbox.com](#)
- [Zune](#)

Related Links

- [Silverlight Privacy Statement](#)
- [Security at Home](#)
- [Trustworthy Computing](#)
- [FTC Privacy Initiatives](#)

By signing in on one Microsoft site or service, you may be automatically signed into other Microsoft sites and services. If you access our services via a mobile phone, you may also use your telephone number and a PIN as an alternative credential to your username and password. As part of creating your credentials, you may also be requested to provide questions and secret answers, which we use to help verify your identity and assist in resetting your password, as well as an alternate e-mail address. Some services may require added security, and in these cases, you may be asked to create an additional security key. Finally, a unique ID number will be assigned to your credentials which will be used to identify your credentials and associated information.

We may collect information about your interaction with Microsoft sites and services. For example, we may use website analytics tools on our site to retrieve information from your browser, including the site you came from, the search engine(s) and the keywords you used to find our site, the pages you view within our site, your browser add-ons, and your browser's width and height. We may also use technologies, such as cookies and web beacons (described [below](#)), to collect information about the pages you view, the links you click and other actions you take on our sites and services. Additionally, we collect certain standard information that your browser sends to every website you visit, such as your IP address, browser type and language, access times and referring Web site addresses. We also deliver advertisements (see the [Display of Advertising](#) section below) and provide Web site analytics tools on non-Microsoft sites and services, and we may collect information about page views on these third party sites as well.

When you receive newsletters or promotional e-mail from Microsoft, we may use web beacons (described below), customized links or similar technologies to determine whether the e-mail has been opened and which links you click in order to provide you more focused e-mail communications or other information.

In order to offer you a more consistent and personalized experience in your interactions with Microsoft, information collected through one Microsoft service may be combined with information obtained through other Microsoft services. We may also supplement the information we collect with information obtained from other companies. For example, we may use services from other companies that enable us to derive a general geographic area based on your IP address in order to customize certain services to your geographic area.

[↑ Top of page](#)

Use of Your Personal Information

Microsoft collects and uses your personal information to operate and improve its sites and services. These uses may include providing you with more effective customer service; making the sites or services easier to use by eliminating the need for you to repeatedly enter the same information; performing research and analysis aimed at improving our products, services and technologies; and displaying content and advertising that are customized to your interests and preferences. For more information about the use of information for advertising, see the [Display of Advertising](#) section below.

We also use your personal information to communicate with you. We may send certain mandatory service communications such as welcome letters, billing reminders, information on technical service issues, and security announcements. Some Microsoft services, such as Windows Live Hotmail, may send periodic member letters that are considered part of the service. We may also occasionally send you product surveys or promotional mailings to inform you of other products or services available from Microsoft and its affiliates.

Personal information collected on Microsoft sites and services may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or service providers maintain facilities. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union.

[↑ Top of page](#)

Sharing of Your Personal Information

Except as described in this statement, we will not disclose your personal information outside of Microsoft and its controlled subsidiaries and affiliates without your consent. Some Microsoft sites allow you to choose to share your personal information with select Microsoft partners so that they can contact you about their products, services or offers. Other sites, such as MSN, do not share your contact information with third parties for marketing purposes, but instead may give you a choice as to whether you wish to receive communications from

Microsoft on behalf of external business partners about a partner's particular offering (without transferring your personal information to the third party). See the Communication Preferences section below for more information.

Some Microsoft services may be co-branded and offered in conjunction with another company. If you register for or use such services, both Microsoft and the other company may receive information collected in conjunction with the co-branded services.

We occasionally hire other companies to provide limited services on our behalf, such as handling the processing and delivery of mailings, providing customer support, hosting websites, processing transactions, or performing statistical analysis of our services. Those service providers will be permitted to obtain only the personal information they need to deliver the service. They are required to maintain the confidentiality of the information and are prohibited from using it for any other purpose. However, for credit card processing, our fraud detection vendors may use aggregate data to help improve their service. This helps them more accurately detect fraudulent uses of credit cards. We may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the services; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers or the public.

[↑ Top of page](#)

Accessing Your Personal Information

You may have the ability to view or edit your personal information online. In order to help prevent your personal information from being viewed by others, you will be required to sign in with your credentials (e-mail address and password). The appropriate method(s) for accessing your personal information will depend on which sites or services you have used.

- **Microsoft.com** - You can access and update your profile on microsoft.com by visiting the [Microsoft.com Profile Center](#).
- **Microsoft Billing and Account Services** - If you have a Microsoft Billing account, you can add to or update your information at the [Microsoft Billing Web site](#) by clicking on the "Personal Information" or "Billing Information" links.
- **Microsoft Connect** - If you are a registered user of Microsoft Connect, you can access and edit your personal information by clicking [Manage Your Connect Profile](#) at the Microsoft Connect Web site.
- **MSN & Windows Live** - If you have used MSN or Windows Live services, you can update your profile information, change your password, view the unique ID associated with your credentials, or close certain accounts by visiting MSN / Windows Live [Account Services](#).
- **MSN Public Profile** - If you have created a public profile on MSN, you may also edit or delete information in your public profile by going to the [MSN Member Directory](#).
- **MSN Keyword Advertising** - If you buy MSN Keyword advertising, you can review and edit your personal information at the [Microsoft adCenter Web site](#).
- **Microsoft Partner Programs** - If you are registered with Microsoft Partner Programs, you can review and edit your profile by clicking [Manage Your Account](#) on the Partner Program Web site.
- **Xbox** - If you are an Xbox Live or Xbox.com user, you can access and edit your personal information on the [My Xbox](#) page on Xbox.com or on your console by selecting Privacy Settings under Edit Gamer Profile on Xbox 360, or selecting the Info Sharing option in Account Management for the Original Xbox Live dashboard.
- **Zune** - If you have a Zune account or a Zune Pass subscription, you can view and edit your personal information at [Zune.net](#) (click Manage My Account from your profile page) or through the Zune software (sign in, click your Zune tag, then click My Account or Privacy Settings to go to the appropriate page at Zune.net).

Some Microsoft sites or services may collect personal information that is not accessible via the links above.

However, in such cases, you may be able to access that information through alternative means of access described by the service. Or you can write us by using our [Web form](#), and we will contact you within 30 days regarding your request.

[↑ Top of page](#)

Communication Preferences

You can stop the delivery of future promotional e-mail from Microsoft sites and services by following the specific instructions in the e-mail you receive.

You may also have the option of proactively making choices about the receipt of promotional e-mail, telephone calls, and postal mail from particular Microsoft sites or services by visiting and signing into the following pages:

- The [Microsoft.com Profile Center](#) allows you to choose whether you wish to receive marketing communications from Microsoft.com, to select whether Microsoft.com may share your contact information with selected third parties, and to subscribe or unsubscribe to newsletters about our products and services.
- The [MSN & Windows Live Communications Preferences](#) page allows you to choose whether you wish to receive marketing material from MSN or Windows Live. You may subscribe and unsubscribe to MSN Newsletters by going to the [MSN Newsletters website](#).
- If you have an Xbox.com or Xbox Live account, you can set your contact preferences and choose whether to share your contact information with Xbox partners on the [My Xbox](#) page on Xbox.com or on your console by selecting Privacy Settings under Edit Gamer Profile on Xbox 360, or selecting the Info Sharing option in Account Management on the Original Xbox Live dashboard.
- If you are registered with Microsoft Partner Programs, you can set your contact preferences or choose to share your contact information with other Microsoft partners by clicking [Manage Your Account](#) on the Partner Program Web site.
- If you have a Zune account or a Zune Pass subscription, you can set your contact preferences and choose whether to share your contact information with Zune partners at [Zune.net](#) (click Manage My Account, Newsletter Options from your profile page) or through the Zune software (sign in, click your Zune tag, then click My Account, Newsletter Options to go to the appropriate page at Zune.net).

These choices do not apply to the display of online advertising. Nor do they apply to the receipt of mandatory service communications that are considered part of certain Microsoft services, which you may receive periodically unless you cancel the service.

[↑ Top of page](#)

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.

[↑ Top of page](#)

Security of Your Personal Information

Microsoft is committed to protecting the security of your personal information. We use a variety of security technologies and procedures to help protect your personal information from unauthorized access, use, or disclosure. For example, we store the personal information you provide on computer systems with limited access, which are located in controlled facilities. When we transmit highly confidential information (such as a credit card number or password) over the Internet, we protect it through the use of encryption, such as the Secure Socket Layer (SSL) protocol.

If a password is used to help protect your accounts and personal information, it is your responsibility to keep your password confidential. Do not share this information with anyone. If you are sharing a computer with anyone you should always log out before leaving a site or service to protect access to your information from subsequent users.

[↑ Top of page](#)

Collection and Use of Children's Personal Information

Many Microsoft sites and services are intended for general audiences and do not knowingly collect any personal information from children. When a Microsoft site does collect age information, and users identify themselves as under 13, the site will either block such users from providing personal information, or will seek to obtain consent from parents for the collection, use and sharing of their children's personal information. We will not knowingly ask children under the age of 13 to provide more information than is reasonably necessary to provide our services.

Please note that if you grant consent for your child to use Microsoft services, this will include such general audience communication services as e-mail, instant messaging, and online groups, and your child will be able to communicate with, and disclose personal information to, other users of all ages. Parents can change or revoke the consent choices previously made, and review, edit or request the deletion of their children's personal information. For example, on MSN and Windows Live, parents can visit Account Services, and click on "Permission for Kids." If we change this privacy statement in a way that expands the collection, use or disclosure of children's personal information to which a parent has previously consented, the parent will be

notified and we will be required to obtain the parent's additional consent.

If you have an MSN Premium, MSN Plus, or MSN 9 Dial-Up account, and use MSN Client software version 9.5 or below, you can choose to set up MSN Parental Controls for the other users of that account. Please read the supplemental privacy information for [MSN](#) for further information. For users of MSN Client software version 9.6 and above, we recommend the use of [Windows Live OneCare Family Safety](#). We also offer an area that is specifically designed for children at <http://kids.msn.com/> which has a special privacy statement that informs children and parents about the MSN Kids area, describes the additional privacy protections provided in this area, and provides children with tips on how to protect themselves online.

We encourage you to talk with your children about communicating with strangers and disclosing personal information online. You and your child can visit our [online safety resources](#) for additional information about using the Internet safely.

[↑ Top of page](#)

Use of Cookies

Microsoft Web sites use "cookies" to enable you to sign in to our services and to help personalize your online experience. A cookie is a small text file that is placed on your hard disk by a Web page server. Cookies contain information that can later be read by a Web server in the domain that issued the cookie to you. Cookies cannot be used to run programs or deliver viruses to your computer.

One of the primary purposes of cookies is to store your preferences and other information on your computer in order to save you time by eliminating the need to repeatedly enter the same information and to display your personalized content and appropriate advertising on your later visits to these sites. Microsoft Web sites also use cookies as described in the [Collection of your Information](#) and [Display of Advertising](#) sections of this privacy statement.

When you sign in to a site using your Windows Live ID or Microsoft Passport Network credentials, we store your unique ID number, and the time you signed in, in an encrypted cookie on your hard disk. This cookie allows you to move from page to page at the site without having to sign in again on each page. When you sign out, these cookies are deleted from your computer. We also use cookies to improve the sign in experience. For example, your e-mail address may be stored in a cookie that will remain on your computer after you sign out. This cookie allows your e-mail address to be pre-populated, so that you will only need to type your password the next time you sign in. If you are using a public computer or do not otherwise want this information to be stored, you can select the appropriate radio button on the sign-in page, and this cookie will not be used.

You have the ability to accept or decline cookies. Most Web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. If you choose to decline cookies, you may not be able to sign in or use other interactive features of Microsoft sites and services that depend on cookies, and some advertising preferences that are dependent on cookies may not be able to be respected.

If you choose to accept cookies, you also have the ability to later delete cookies that you have accepted. In Internet Explorer 7, you can delete cookies by selecting "Tools", "Delete browsing history" and clicking the "Delete Cookies" button. If you choose to delete cookies, any settings and preferences controlled by those cookies, including advertising preferences, will be deleted and may need to be recreated.

[↑ Top of page](#)

Use of Web Beacons

Microsoft Web pages may contain electronic images known as Web beacons - sometimes called single-pixel gifs - that may be used to assist in delivering cookies on our sites and allow us to count users who have visited those pages and to deliver co-branded services. We may include Web beacons in promotional e-mail messages or our newsletters in order to determine whether messages have been opened and acted upon.

Microsoft may also employ Web beacons from third parties in order to help us compile aggregated statistics regarding the effectiveness of our promotional campaigns or other operations of our sites. We prohibit Web beacons on our sites from being used by third parties to collect or access your personal information.

Finally, we may work with other companies that advertise on Microsoft sites to place Web beacons on their sites in order to allow us to develop statistics on how often clicking on an advertisement on a Microsoft site results in a purchase or other action on the advertiser's site.

[↑ Top of page](#)

Controlling Unsolicited E-mail ("Spam")

Microsoft is concerned about controlling unsolicited commercial e-mail, or "spam." Microsoft has a strict [Anti-Spam Policy](#) prohibiting the use of a Windows Live Hotmail or other Microsoft-provided e-mail account to send spam. Microsoft will not sell, lease or rent its e-mail subscriber lists to third parties. While Microsoft continues to actively review and implement new technology, such as expanded filtering features, there is no currently available technology that will totally prevent the sending and receiving of unsolicited e-mail. Using junk e-mail tools and being cautious about the sharing of your e-mail address while online will help reduce the amount of unsolicited e-mail you receive.

[↑ Top of page](#)

TRUSTe Certification

Microsoft is a member of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build trust and confidence in the Internet by promoting the use of fair information practices. To demonstrate our commitment to your privacy, we have agreed to disclose our information practices and have our privacy practices reviewed for compliance by TRUSTe. The TRUSTe program covers only information that is collected through Microsoft's Web sites, and does not cover information that may be collected through software downloaded from such sites.

[↑ Top of page](#)

Enforcement of This Privacy Statement

If you have questions regarding this statement, you should first contact us by using our [Web form](#). If you do not receive acknowledgement of your inquiry or your inquiry has not been satisfactorily addressed, you should then contact TRUSTe at http://www.truste.org/consumers/watchdog_complaint.php. TRUSTe will serve as a liaison with Microsoft to resolve your concerns.

[↑ Top of page](#)

Changes to This Privacy Statement

We will occasionally update this privacy statement to reflect changes in our services and customer feedback. When we post changes to this Statement, we will revise the "last updated" date at the top of this statement. If there are material changes to this statement or in how Microsoft will use your personal information, we will notify you either by prominently posting a notice of such changes prior to implementing the change or by directly sending you a notification. We encourage you to periodically review this statement to be informed of how Microsoft is protecting your information.

[↑ Top of page](#)

Contacting Us

Microsoft welcomes your comments regarding this privacy statement. If you have questions about this statement or believe that we have not adhered to it, please contact us by using our [Web form](#). If you have a technical or general support question, please visit <http://support.microsoft.com> to learn more about Microsoft Support offerings.

Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052 USA • 425-882-8080

To find the Microsoft subsidiary in your country or region, see <http://www.microsoft.com/worldwide/>.

© 2008 Microsoft Corporation. All rights reserved. [Anti-Spam Policy](#)

[↑ Top of page](#)

[Manage Your Profile](#) | [Contact Us](#) | [Microsoft This Week! Newsletter](#) | [Legal](#)

© 2008 Microsoft Corporation. All rights reserved. [Contact Us](#) | [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

Appendix 3: Privacy Protections in Microsoft's Ad
Serving System and the Process of "De-identification"

Privacy Protections in Microsoft's Ad Serving System and the Process of "De-identification"

As part of its strong commitment to protecting individual privacy,
by design Microsoft bases its ad selection solely on data that
does not personally and directly identify individual users.

Microsoft Corporation

October 2007

The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of Microsoft.

Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

© 2007 Microsoft Corp. All rights reserved.

Microsoft, Hotmail, MSN, Windows, Windows Live and Windows Vista are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

Introduction

As the Internet has matured, online advertising has become the means by which many Web sites offer users rich content and services for free. Online advertising has also become an increasingly sophisticated vehicle for targeting users' interests—based on context (such as car ads on a car Web site) or based on user behavior on a site. The serving of relevant ads benefits advertisers, who are more likely to find customers for their products. It also benefits consumers, who are less likely to see ads that do not interest them. The key is making sure that users' privacy is protected in the process.

As part of its strong commitment to protecting individual privacy, by design Microsoft bases its ad selection solely on data that does not personally and directly identify individual users. The vast majority of ads that Microsoft serves online are not targeted to specific known users—they are based on context or are untargeted. For individually targeted ads, Microsoft's ad serving platform stores the data used for ad personalization separate from contact information or any other data that directly identifies the user. The system also has strong built-in safeguards against unauthorized correlation of these sets of data. The key to these important privacy protections is the use of an "Anonymous" ID (ANID) to enable recording of relevant online user activity without correlating it with data that can be used to personally and directly identify a user. This paper describes how Microsoft uses the ANID as a part of the de-identification process it uses to achieve robust individual privacy protections while still serving relevant targeted ads to users of its Web sites and online services, including MSN® and Windows Live™ sites.

Overview of Ad Targeting

Generally, online ad targeting providers try to correlate the interests of users, as implied by their past behavior or demographics, with the ads those users are served. Users' perceived interests are inferred over time based on information they provide when they register with a Web site or service or actions they take and information they provide when interacting with the site or service. In some cases, their interests are also inferred using publicly available information supplied by third parties. Based on this collection of data, users are assigned to different targeting segments and are accordingly served segment-specific ads. Users can be targeted in this way without the advertiser having any information that might personally and directly identify an individual person. (Similar kinds of behavioral targeting have existed in the offline direct mail and telemarketing industries for years, although they generally require identifying information such as names, mailing addresses and telephone numbers.)

A generic per-computer ad targeting scenario typically works in the following way: A user visits a Web site, and the site places a cookie on the user's computer. A cookie is a tiny text file into which a Web site stores information called a cookieID that it can later use to recognize the user. The cookieID is also recorded in a database at the Web site. Let's assume that the user is visiting the site for the first time and that he has not and will not register at the site or provide the site with any information that could personally and directly identify him. The user is therefore unknown to the site. Each time the user visits that site, the site reads the cookieID and logs his actions on the site. These actions are stored in the database by the Web server and associated with the cookieID. Over time, the cookieID entries in the database might build up a significant record of actions taken by the unknown user on the site.

When sufficient data has been collected, the Web site's business rules might place the cookieID into one or more segments based on the user actions logged in the database. For example, if a user visits the hotel portion of a travel Web site often enough, the cookieID associated with his computer might be placed into a "Hotel Seekers" buying segment. From that point until the business rules dictate differently, the user might be shown hotel ads when he visits that site. Such behavioral targeting has been shown to significantly increase click-through and conversion rates for advertisers.

Clearing the cookie on the user's computer disassociates that computer from the cookieID and the logs of the user's behaviors and segments on the Web site's database. If the user never clears the cookie, the cookie will persist on his computer and the site can continue to accrue information until the cookie's expiration date or until the computer is recycled or the operating system is reinstalled or replaced.

This scenario becomes somewhat more complicated if a computer or computer user account is shared by two or more people. In general, a separate set of cookies is created for each user account (an account with a separate username and password) on a computer. In the case of Microsoft® Windows Vista® or Windows® XP, if all users of a PC share a single user account, the cookies stored on that PC may represent the totality of all their actions on that computer. So, for example, the records that a Web site attributes to a single unknown user might actually represent the actions of an entire family that shares the same computer account or the actions of all users of a public computer. If each user of the PC uses a separate account, each user will have a separate set of cookies.

Third-party ad networks—service providers that provide ads to a number of Web sites—serve targeted ads to computers in a manner similar to that just described. However, they differ in two significant ways. First, ad networks generally have broader reach because they serve ads

across a variety of (often unrelated) Web sites rather than on a single site. Second, they may aggregate information about a user's behavior across multiple sites on which they serve ads, so they might capture a broader range of user activity.

Ad Targeting at MSN and Windows Live¹

As a matter of policy, Microsoft takes steps to separate any information that can be used to personally and directly identify a user—such as name, e-mail address or phone number—from the information in its ad selection system. This de-identification adds an important layer of privacy protection while still allowing Microsoft to serve targeted ads based on user behavior. In other words, the MSN and Windows Live sites do not need to correlate personally and directly identifying data with user behavior online in order to take full advantage of behavioral targeting. For example, MSN can target ads to a person who likes coffee, lives in Seattle and is male without knowing the name, e-mail address or any other personally identifying information that the user might have provided when registering for particular services on MSN or Windows Live.

Microsoft uses three different cookies—the Machine Unique ID (MUID), the Windows Live User ID (LiveID) and the “Anonymous” ID (ANID)—in its ad targeting infrastructure.² The latter two are part of the process that segregates data used for ad personalization from information that could personally and directly identify a user. We'll look at each of these in turn.

The Machine Unique ID (MUID)

When a user first visits an MSN or Windows Live site, a standard cookie with a randomly generated unique identifier called the Machine Unique ID (MUID) is placed on the user's computer (the “machine”). For the purpose of ad targeting, that cookieID may behave in the same manner as the cookieID described earlier in the generic example. This means that the MUID may be used to target ads based on the behaviors of an unknown user. This behavior is illustrated in Figure 1. Information that could personally and directly identify a user is not associated with the MUID.

¹ This paper does not cover Microsoft's newly acquired Atlas ad serving technology.

² Microsoft sites might set other cookies for other purposes, but they are not relevant to the online advertising topics described here and are therefore not discussed in this paper.

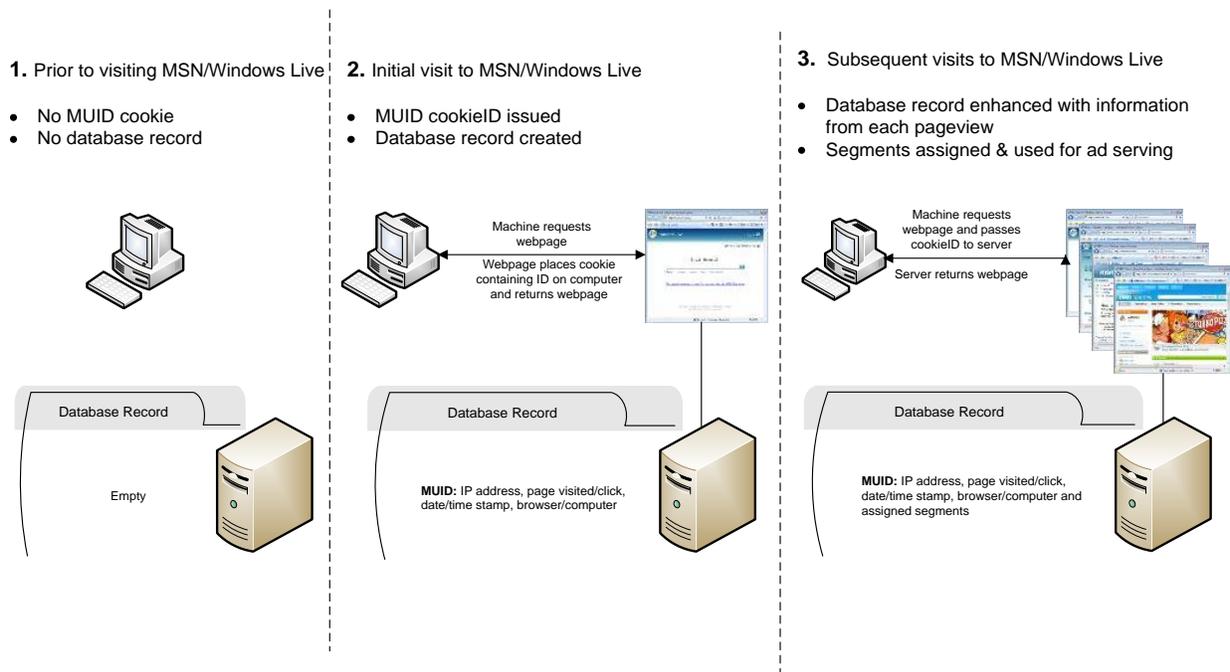


Figure 1. The Machine Unique ID (MUID).

The Windows Live User ID (LiveID)

The example of the MUID involves a cookieID that is assigned per computer account to users who are not known to the Web site. Now we'll discuss cookieIDs that are assigned on a "per-login" basis to users who have established a relationship with the Web site.

In general, Web sites that require a user to log in to access a user-specific service, such as Web-based e-mail, use a user-based cookieID as a part of their system for granting access. At MSN and Windows Live, the core user-based ID is the Windows Live ID (LiveID). When a user first registers at the site, she typically chooses a username and password and provides Microsoft with a first and last name, plus a few pieces of non-identifying demographic information such as country, Zip code, age, gender and language. In scenarios where a user is creating a billing account, additional pieces of personal information might also be collected at this point. A unique LiveID is then generated and associated with this data. The LiveID is the unique ID number specific to that user account.

The LiveID is stored on the Windows Live ID servers and, once the user has presented a valid username and password, is placed in a cookie on her computer. The presence of the LiveID cookie is the signal to an MSN or Windows Live service that it should continue to grant access—for example, to the user's e-mail in the case of Windows Live Hotmail. When the user logs out of the service or ends the session, the LiveID cookie expires (unless the user has opted to make

the cookie permanent by clicking “Save My Password” so she does not have to log in each time she accesses the service). Granting a user access to her Hotmail e-mail is an example of when the LiveID needs to be associated with personal information. Other Windows Live services that require this type of authentication via a LiveID include Windows Live Messenger and Windows Live Spaces.

Because the LiveID database contains data that could be used to personally and directly identify individual users, by design Microsoft’s advertising system *does not* use the LiveID to select and serve ads—even though it would be technically far simpler to have it do so. One of Microsoft’s [online advertising principles](#) is that its ad targeting platform can select appropriate ads based *only* on data that does not personally and directly identify individual users.³

The “Anonymous” ID (ANID)

One of Microsoft’s goals is to serve targeted ads in a manner that protects user privacy. To avoid using the LiveID cookie to serve per-user ads—because, as described earlier, it is directly associated with information that could personally identify the user—Microsoft has created an “Anonymous” ID, called the ANID, on which its ad serving capabilities are based.

When a user first registers with Windows Live or MSN, a LiveID and an ANID are created simultaneously. The ANID is derived by applying a one-way cryptographic hash function to the LiveID. A one-way cryptographic hash function ensures that there is no practical way of deriving the original value from the resulting hash value—that is, the process cannot be reversed to obtain the original number.

What this means in practical terms is that each time a registered user logs in, Microsoft’s system applies the hash function to the LiveID to generate an ANID, and each ID is put in a separate cookie on the computer. The advantage of using a one-way cryptographic hash function is that although the same number is guaranteed to be generated each time it is applied to a given LiveID, it is virtually impossible to reverse the process. In other words, it is extremely difficult to use a given ANID (with or without knowing the hashing algorithm) to derive the original LiveID value. Because all personally and directly identifying information about a user is stored on servers in association with a LiveID rather than an ANID, there is no practical way to link data stored in association with an ANID back to any data on Microsoft

³ Microsoft’s online advertising principles can be found at <http://download.microsoft.com/download/3/7/f/37f14671-ddee-499b-a794-077b3673f186/Microsoft's%20Privacy%20Principles%20for%20Live%20Search%20and%20Online%20Ad%20Targeting.doc>.

servers that could personally and directly identify an individual user. Figure 2 illustrates this relationship between the two IDs.

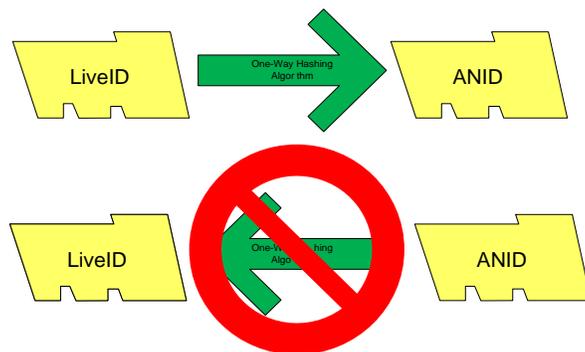


Figure 2. One-way cryptographic hash.

As mentioned earlier, a user might input particular pieces of demographic information when a LiveID is created. When the LiveID and ANID are created, the demographic information that cannot be used to personally and directly identify the user is copied to a database that is indexed on only the ANID. Microsoft's ad serving infrastructure consumes data associated with the ANID but not the LiveID, so copying the demographic data in this way allows Microsoft to make it available to the ad serving infrastructure. As a user with an ANID cookie on her computer navigates around the Microsoft sites, data associated with her online behaviors, such as searches and pageviews, is associated with the ANID. All of this information can then be used to assign ad targeting segments to the ANID in the same manner as described previously in the generic description of ad targeting. (Figure 3 illustrates this process.) Most importantly, because of the one-way hash used in creating the ANID, none of the specific behaviors associated with the ANID or the ad targeting segments consequently assigned to the ANID are linked back to the personal information associated with the LiveID.

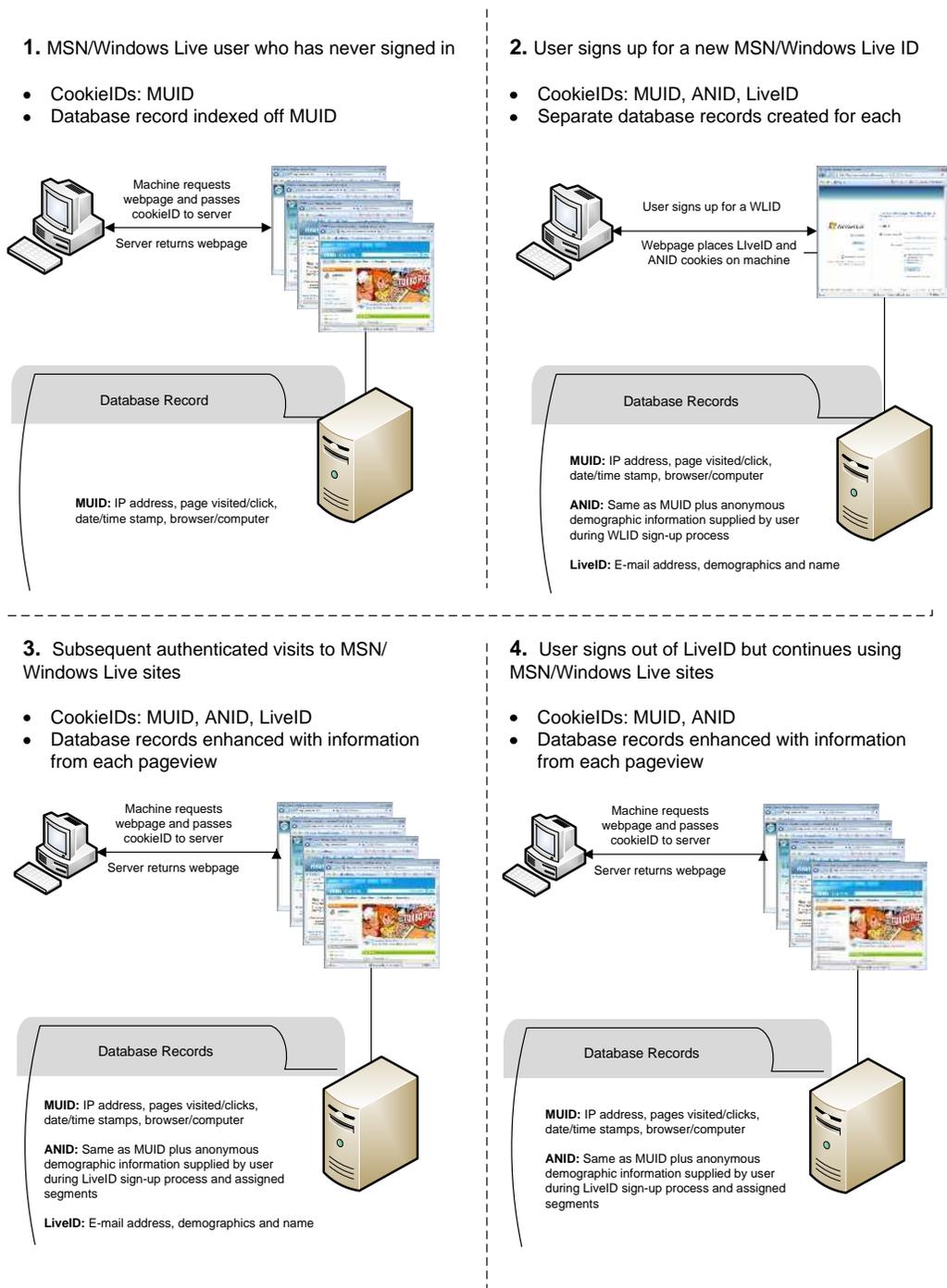


Figure 3. Sample MUID, ANID and LiveID interactions.

When a user logs out of a Windows Live account, the LiveID cookie is deleted from her computer. However, the ANID cookie remains on the user's system until a different Windows Live account is accessed from that computer account (which would replace the old ANID cookie

with a different one), until the user takes steps to delete the ANID cookie or until the cookie expires.

Privacy protections tend to be strongest when implemented as a part of the fundamental architecture of a computer system. Microsoft's ad serving system was designed expressly to work with the ANID, and the ANID was designed expressly to enhance user privacy. These safeguards help ensure that information associated with a LiveID will not leak into the ad serving environment.

Of course, the ANID infrastructure itself does not guarantee complete and irreversible anonymity. But it does provide strong technical protection, which, combined with stringent internal policies, is designed to keep the data used for ad serving separated from information that identifies an individual.

For example, because the system is ANID-based, Microsoft employees with access to the company's ad serving system alone cannot identify users who are served ads based on the data in the system. Furthermore, to associate any of the ANID-based data in the Microsoft ad system with an individual user, an internal or external attacker would not only need access to the ad serving system (to access the data), the Windows Live ID system (to access all LiveIDs ever issued) and the hashing algorithm but would also need a massive computing infrastructure to run the algorithm on each and every LiveID ever created to try to find the ANID in question. Each of these components is separately protected with strong internal security measures, rendering this scenario virtually impossible.

Further, the use of the ANID is part of the company's overall approach to protecting user privacy, which includes strong and meaningful protections from the time that behavioral data is first collected. These protections also include the recently announced policy of anonymizing search query data after 18 months. (This includes the complete and irreversible deletion of full IP addresses and cookieIDs—including ANIDs—from search terms.)

Conclusion

Microsoft's use of the ANID enables the delivery of relevant ads to users while basing ad selection solely on data that does not personally and directly identify individual users. As a fundamental element of Microsoft's ad targeting infrastructure, the ANID underscores the company's strong commitment to privacy. It is complemented by the recent announcement of

Microsoft's [Privacy Principles for Live Search and Online Ad Targeting](#),⁴ the public release of the company's [Privacy Guidelines for Developing Software Products and Services](#)⁵ and its advocacy for comprehensive federal privacy legislation in the United States and strong public policies worldwide to protect consumer privacy. In a dynamic industry where rules and best practices are continually evolving, Microsoft is committed to ensuring that its current and future products and services implement industry-leading technologies and processes that protect individual privacy.

⁴ Available at <http://download.microsoft.com/download/3/7/f/37f14671-ddee-499b-a794-077b3673f186/Microsoft's Privacy Principles for Live Search and Online Ad Targeting.doc>.

⁵ Available at <http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83EC-A18D1AD2FC1F&displaylang=en>.

Appendix 4: Microsoft's Comments to the Federal Trade
Commission



April 11, 2008

VIA HAND AND EMAIL DELIVERY

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles

Dear Secretary Clark:

Microsoft submits these comments in response to the Commission's request for feedback on its proposed self-regulatory principles for online behavioral advertising. Microsoft commends the Commission for releasing these principles and for its successful November Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology." The Commission's efforts have raised awareness and fostered an important dialogue among stakeholders about the privacy issues associated with online advertising.

I. EXECUTIVE SUMMARY

Microsoft recognizes the need for self-regulatory principles governing online advertising that provide consumers with greater transparency and control. Microsoft's own online advertising practices include commitments to user notice, user control, anonymization, security, and best practices. These principles are generally tailored to account for the types of information we collect and how we intend to use that information. Microsoft suggests that the Commission adopt a similarly nuanced approach to its self-regulatory principles that impose increasing obligations depending on the type of online advertising activity involved:

- Any entity that logs page views or collects other information about consumers for the purpose of delivering ads or providing advertising-related services ("online advertising") within its own site should inform consumers of its advertising practices in a privacy notice that is available through a clear and conspicuous link on its site's homepage, implement reasonable security procedures, and retain data only as long as necessary to fulfill a legitimate business need or as required by law.

- Third parties that collect information about consumers for online advertising across multiple, unrelated third-party sites (“multi-site advertising”) should take reasonable steps to ensure consumers receive notice of their activities.
- Third parties that seek to develop a profile of consumer activity to deliver advertising across multiple, unrelated third-party sites (“behavioral advertising”) should additionally offer consumers a choice about the use of their information for such purposes.
- Third parties seeking to merge personally identifiable information with information collected through multi-site or behavioral advertising should be subject to additional obligations.
- Third parties should be required to obtain affirmative express consent before using sensitive personally identifiable information for behavioral advertising.

The increasing obligations that should flow from the type of advertising activity involved can be summarized as follows:

Type of Advertising	Definition	Obligation
Sensitive Personally Identifiable Information Advertising	The use of sensitive personally identifiable information for the purpose of behavioral advertising.	Opt-in consent
Personally Identifiable Advertising	The merger of information that, by itself, can be used to identify someone – such as name, e-mail address, physical address, or telephone number – with data collected through multi-site or behavioral advertising for the purpose of ad targeting.	Opt-in consent
Behavioral Advertising	The tracking of a consumer’s activities online across multiple, unrelated sites – including the searches the consumer has conducted, the web pages visited, and the content viewed – by a third party in order to deliver advertising across multiple, unrelated sites targeted to the individual consumer’s interests.	Opt-in consent
Multi-site Advertising	Online advertising across multiple, unrelated third-party sites.	Pass reasonable operators make website notice on
Online Advertising	The logging of page views or the collection of other information about an individual consumer or computer for the purpose of delivering ads or providing advertising-related services.	Link to p follow re

In addition, with respect to material changes, the Commission should clarify that the level of notice and consumer consent required depends on various factors, including the materiality of the change and whether it would apply retroactively or prospectively.

II. INTRODUCTION

Online advertising has assumed a large and growing significance in global economies. As the Commission recognizes, online advertising enables advertisers to target their ads to specific consumers and allows consumers to receive ads that they are more likely to find useful. This facilitates comparison shopping, reduces the number of irrelevant ads received by consumers, and subsidizes the wide variety of free content and services available to consumers online. Consumers value these benefits, but, as the Commission notes, they may not fully appreciate the role that data collection plays in providing them. They also may not appreciate other elements of online advertising that may impact their privacy — most notably that third parties may be involved in delivering online ads and collecting information about them.

In light of these concerns, Microsoft announced five fundamental privacy principles last July for online search and ad targeting. These principles touch upon many of the same themes as those addressed by the Commission and include commitments to user notice, user controls, anonymization, security, and best practices. These principles are discussed in greater detail below, and a full copy of the principles is attached to these comments. Late last year, Microsoft also began the process of joining the Network Advertising Initiative (“NAI”), a cooperative of online marketing and advertising companies that addresses important privacy and consumer protection issues in emerging media.¹

Microsoft’s efforts in the online advertising area are just one aspect of our broader commitment to protecting consumer privacy. We were one of the first companies to advocate for comprehensive federal privacy legislation in the United States. We have led the industry in adopting privacy notices that are clear, concise, and understandable. We have released a set of privacy guidelines designed to help developers build meaningful privacy protections into their software programs and online services.² And 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.

Microsoft welcomes the opportunity to provide comment on the Commission’s proposed self-regulatory framework. Our comments begin by providing an overview of the online advertising principles Microsoft has committed to follow. We then propose a multi-tiered self-regulatory approach that should apply to all entities engaged in advertising online, and we discuss the reasonable security and limited data retention procedures that such entities should follow. We also provide input on the Commission’s proposal around material changes and finally respond to the Commission’s request for additional information about using tracking data for purposes other than online advertising.

¹ Atlas, a Microsoft subsidiary, was a founding member of NAI and remains a member.

² Microsoft’s Privacy Guidelines for Developing Software Products and Services are available at <http://www.microsoft.com/privacy>.

III. MICROSOFT'S ONLINE ADVERTISING PRACTICES

Microsoft's efforts to protect consumer privacy in the online advertising space are reflected in Microsoft's Privacy Principles for Live Search and Online Ad Targeting. These principles build upon existing policies and practices, as reflected in Microsoft's privacy statements, and will help shape the development of our new product offerings. We hope that the insight we have developed in formulating and implementing these principles is of use to the Commission as it contemplates a self-regulatory framework for online advertising.

A. Principle I: User Notice

Microsoft has long believed that providing transparency about its policies and practices is critical to enable consumers to make informed choices. To this end, Microsoft's Online Privacy Statement is readily accessible from every page of each major online service that we operate. It also is written in clear language and offered in a "layered" format that provides consumers with the most important information about our privacy practices upfront, followed by additional layers of notice that provide a more comprehensive examination of our general privacy practices.³ We recently updated our U.S. privacy statement to provide additional detail about the use of information collected through search and page views for ad targeting, and we intend to further update our privacy statement in the near term to provide more information about online advertising and our search data retention practices.

B. Principle II: User Control

Microsoft currently offers consumers a series of controls that enable users to manage the types of communications they receive. As an initial matter, we have built user controls — including control over third-party cookies — into our Internet Explorer product. We also allow users to easily access and edit their stored personal information and to choose the types of e-mail, phone or fax communications they wish to receive from Microsoft.

In addition, we currently offer users the ability to opt out from receiving behaviorally targeted ads through our Atlas subsidiary.⁴ We will soon offer users a choice about receiving targeted ads across both third-party websites and Microsoft-operated websites. We also will enable users to tie their opt-out choice to their Windows Live ID so that their opt-out selection will apply across multiple computers, and if their cookies are deleted, their choice will be reset when they sign in with their ID.

³ For a layered privacy notice to be effective, the top layer should set forth, in plain terms, all important information pertaining to the use, collection, or disclosure of data, including that data is used for behavioral advertising purposes. For example, the Microsoft Online Privacy Notice Highlights informs users that Microsoft "use[s] cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience" and that Microsoft's services "may include the display of personalized content and advertising." Not all companies purporting to follow a layered approach disclose this kind of important information in the initial layer.

⁴ The Atlas opt out is a standard cookie-based opt out.

C. Principle III: Search Data Anonymization

Microsoft has committed to make search query data anonymous after 18 months by permanently removing cookies, the entire IP address, and other identifiers from search logs, unless the user has provided consent for us to retain data for a longer period of time. We made the decision early on that partial approaches — such as removing only portions of an IP address — are inadequate. A partially redacted IP address can still narrow down the field of computers from which an associated search originated. Moreover, an IP address is unlikely to be the only unique identifier associated with search data. Depending upon how the search service is designed, there are likely to be other cookie or machine-based identifiers linked to search data, and some of these identifiers may directly or indirectly correlate to user accounts or other personally identifiable information. The presence of cross-session identifiers could permit the correlation of sufficient search data related to an individual user to make it possible to identify such an individual even without an IP address or without what would traditionally be considered personally identifiable information.⁵ Thus, we believe that, in order to fully protect privacy and make search query data truly anonymous, all cross-session identifiers must be removed in their entirety from the data.

D. Principle IV: Minimizing Privacy Impact and Protecting Data

Microsoft strives to design all systems and processes in a manner that minimizes their negative privacy impact from the outset, while simultaneously promoting security. Microsoft collects (and will continue to collect) only a limited amount of information from Windows Live users — specifically, name, e-mail, password, and demographic data (gender, birth year, country/region, and zip).

We also take steps to separate the data used for ad targeting from any personally identifiable information before using it to serve ads — a process we refer to as “de-identification.” Specifically, for users who have created Windows Live accounts, rather than using the account ID as the basis for our ad systems, we use a one-way cryptographic hash to create a new anonymized identifier. We then use that identifier, along with the non-identifiable demographic data, to serve ads online. Search query data and web surfing behavior used for ad targeting is associated with this anonymized identifier rather than an account identifier that could be used to personally and directly identify a user. In short, user privacy is not only protected through the de-identification process at the outset, but after 18 months, the information is completely and irreversibly anonymized. We believe this multifaceted approach to protecting search query data demonstrates Microsoft’s strong commitment to consumer privacy. A white paper describing Microsoft’s “de-identification” process is attached to these comments.

⁵ Reporters have demonstrated the potential ease with which a series of search queries, linked together by a common identifier, can be associated with specific users. See Michael Barbaro & Tom Zeller Jr., “A Face is Exposed for AOL Searcher No. 4417749,” N.Y. Times, Aug. 9, 2006, at A1 (reporting that “[i]t did not take much investigating” to identify a specific user from the search log entries that AOL released).

Finally, we have implemented robust security protections to prevent the unauthorized correlation of this information and to help protect the information we collect and maintain.

E. Principle V: Legal Requirements and Industry Best Practices

Microsoft adheres to all applicable legal requirements as well as leading industry best practices regarding consumer privacy in all markets where we operate. To this end, Microsoft currently abides by the standards set forth in the Organization for Economic Cooperation and Development (OECD) privacy guidelines, the Online Privacy Alliance (OPA) guidelines, the EU-US Safe Harbor Framework, and the TRUSTe Privacy Program. Microsoft also has advocated for comprehensive federal privacy legislation as an additional pillar of the foundation needed to protect consumer privacy.

IV. SELF-REGULATORY PRINCIPLES SHOULD APPLY TO ALL TYPES OF ONLINE ADVERTISING

Microsoft supports the Commission's intent to encompass a wide variety of activities through its definition of behavioral advertising. We also agree with the Commission that behavioral advertising raises "unique" concerns that may necessitate heightened transparency and control obligations. That said, we believe that the Commission's focus on behavioral advertising is too narrow because it fails to capture the full array of online advertising activities, all of which have potential privacy implications and some of which may be contrary to consumers' expectations. Microsoft suggests a more nuanced approach to self regulation, one that recognizes the varied forms of online advertising and is appropriately tailored to account for the types of information being collected and how that information will be used. To this end, we propose that certain baseline obligations apply to any entity engaged in online advertising, with additional obligations applying if the entity is engaged in multi-site advertising, behavioral advertising, personally identifiable advertising, or sensitive personally identifiable information advertising.

A. Entities engaged in online advertising activities should be transparent about their practices and protect the data they collect.

Consumers may not understand the types of information that entities rely upon to provide advertisements online. For example, many consumers may not realize that information about the pages they are viewing, the searches they are conducting, or the services they are using may be collected and used to deliver online ads. Therefore, Microsoft believes that any entity that logs page views or collects other information about an individual consumer or computer for the purpose of delivering advertisements online should be transparent about its practices.

To this end, the self-regulatory principles should impose some minimal obligations on any entity engaged in "online advertising." We suggest defining online advertising as "the logging of page views or the collection of other information about an individual consumer or computer for the purpose of delivering ads or providing advertising-related services." The following obligations should be imposed on an entity that engages in online advertising:

1. Post a clear and conspicuous link on the home page of its website to a privacy notice that sets forth its data collection and use practices related to online advertising. Such notice should describe, at a minimum, the types of information collected for online advertising; whether this information will be combined with other information collected; and the ways in which such information may be used, including whether any non-aggregate information may be shared with a third party.
2. Take reasonable steps to protect the security of the data it collects for online advertising and retain data only as long as is necessary to fulfill a legitimate business need or as required by law.⁶

B. Third parties engaged in online advertising across multiple, unrelated sites should ensure consumers receive notice of their activities.

Many websites rely on third parties to deliver online advertising. Where third parties deliver ads online, the same transparency concerns discussed above are intensified. This is because the collection of data (e.g., page(s) visited, day and time of visit, IP address, or unique identifier) by a third party with whom they may not have a relationship may not be expected or understood by consumers. If the consumer is not able to determine whether a third party will collect information on a particular site, the consumer cannot make a meaningful decision as to whether to continue using the website. Therefore, consumers should be provided with notice anytime a third party will be collecting information about them to deliver advertisements online.

For these reasons, Microsoft urges the Commission to consider an additional tier of online advertising — “multi-site advertising” — and to define it as “online advertising across multiple, unrelated third-party sites.” To ensure consumers receive notice of these activities, a third party engaged in multi-site advertising should:

1. Make reasonable efforts to require that those websites on which it engages in online advertising post a link on their sites’ homepage to a privacy notice that discloses the use of a third party for online advertising.⁷ This “pass-through notice” approach will have the additional benefit of obligating entities engaged in multi-site online advertising to take some

⁶ These security and retention obligations are discussed in more detail in section V below.

⁷ Obviously, an entity that has a direct contractual relationship with the website on which the ads are served should include the “pass-through notice” as part of the contract. There are other scenarios in which there is not a direct contractual relationship between the entity serving the ads and the website on which the ads are served. In these less direct scenarios, “reasonable efforts” may be accomplished through other means of encouraging best practices among website publishers. Microsoft is committed to working with others in industry to ensure best practices become part of the online advertising ecosystem. In the meantime, references to “pass-through notice” in these comments should be understood to recognize this distinction.

basic steps to require that their website partners at least adhere to the minimal privacy practice of having a privacy notice available via their home pages.

2. Ensure that all pass-through notices describe consumers' right to opt out to the extent the third party engages in behavioral advertising or personally identifiable advertising (as defined below).

C. Third parties engaged in behavioral advertising should offer consumers a choice about the use of their information for such purposes.

Microsoft agrees with the Commission that the collection of information about consumers to generate a profile of their behavior upon which ads can be targeted raises heightened concerns that warrant additional levels of user control. That said, we believe those concerns are most pronounced when a third party engages in targeting ads based on a behavioral profile developed across multiple, unrelated sites. In its 2000 Report to Congress on issues associated with online profiling, the Commission noted the “widespread concern” regarding profiling practices by companies with whom users do not have a “known, direct relationship.”⁸ Proposed state legislative efforts around behavioral advertising have similarly focused on third parties,⁹ and State Attorneys General have set parameters around the development of behavioral profiles by companies with whom consumers lack an established relationship.¹⁰

In contrast, the delivery of advertising by a company on its own website, or within a closely-related family of websites,¹¹ based on information collected within that site raises limited privacy concerns.¹² Certainly this online advertising activity should be disclosed in the

⁸ See *Online Profiling: A Report to Congress*, June 2000, available at <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>; see also FTC Statement Before the Committee on Commerce, Science, and Transportation, United States Senate, “Online Profiling: Benefits and Concerns,” June 13, 2000, available at <http://www.ftc.gov/os/2000/06/onlineprofile.htm> (noting “persistent concern[s]” regarding the “extensive and sustained scope of the monitoring”).

⁹ See, e.g., Assemb. 9275-B, 2007-2008 Reg. Sess. (N.Y. 2008) (“Third Party Internet Advertising Consumers’ Bill of Rights”).

¹⁰ See *DoubleClick Consent Order*, available at http://www.oag.state.ny.us/press/2002/aug/aug26a_02_attach.pdf (requiring companies engaged in online preference monitoring across multiple sites to disclose their activities to consumers).

¹¹ Websites should be considered “closely related” where a reasonable consumer would understand that the sites are owned and operated by the same entity.

¹² The Commission should consider whether there are some online advertising activities even within the scope of a single website or online service — such as serving ads based on the content of email communications or documents stored on consumers’ hard drives — that are so personal or sensitive as to require additional obligations (such as requiring entities to offer users choice before using the contents of email communications to serve ads). Although this issue is outside the Commission’s request for feedback, we would be happy to engage in a discussion with the Commission on these other scenarios.

privacy policy posted on the site’s homepage, as required by the principles around online advertising noted above. But it is simply less invasive than the collection of information across multiple, unrelated sites by a third party with whom the consumer may not have a relationship in an effort to generate a profile of user behavior upon which ads can be targeted. Consumers should be able to choose whether or not to have their information collected and used for such purposes.

Accordingly, Microsoft urges the Commission to modify its definition of “behavioral advertising” to focus on third-party tracking across multiple, unrelated sites:

“The tracking of a consumer’s activities online across multiple, unrelated sites — including the searches the consumer has conducted, the web pages visited, and the content viewed — by a third party in order to deliver advertising across multiple, unrelated sites targeted to the individual consumer’s interests.”

We believe a third party engaged in behavioral advertising should take the following additional steps:

1. Enable consumers to choose not to have their information used for behavioral advertising.
2. Respect consumers’ opt-out choice on all sites where it engages in behavioral advertising. This is important because consumers acting reasonably under the circumstances would expect that the opt-out choice offered by the third party would apply in all circumstances where the third party engages in behavioral advertising practices — not just on sites the third party does not own or control. Indeed, to offer consumers a choice about having their information collected for behavioral advertising but limit that choice to only those sites the third party does not own or control would likely mislead consumers as to the effect of their opt-out choice.¹³
3. Ensure that all privacy notices include clear descriptions of the procedure for consumers to opt out of having their information used for behavioral advertising (including a description of the circumstances that would make it necessary for a consumer to renew the opt out, such as when a consumer changes computers, changes browsers, or deletes relevant cookies) and a link to a place where consumers can exercise such choice. This includes

¹³ This may not be true in every case. There may be discrete programs for which receiving behaviorally targeted ads is a clear condition of using the service and treating the program separately from the third party’s general opt-out opportunity would not confuse consumers. In general, Microsoft believes a third party engaged in behavioral advertising should only determine not to offer consumers an opt-out opportunity from behavioral advertising with respect to its own sites or services in those instances where a reasonable consumer would expect (based on notices received or other factors) that their general decision to opt out of behavioral advertising from the third party would not apply.

pass-through notices, which means third parties should take reasonable steps to require website operators to notify consumers of their ability to exercise choice about the use of their information for behavioral advertising.

D. Third parties seeking to merge personally identifiable information with data collected through multi-site or behavioral advertising should be subject to additional obligations.

The merger of personally identifiable information with other information collected about consumers through multi-site or behavioral advertising for the purposes of ad targeting presents further privacy risks. This is because consumers are unlikely to expect that a third party may combine such pieces of information and use it to deliver ads (whether online or offline). These risks are particularly salient when considered in light of the evolving relationship between consumers and third parties who engage in multi-site and behavioral advertising. Today, unlike in the past, the majority of these companies are owned by entities that provide a wide array of Web-based services and, therefore, often have direct relationships with consumers. This increases the potential that data collected through multi-site or behavioral advertising will be combined or associated with personally identifiable information.

Accordingly, self-regulatory principles should impose heightened obligations on any third party seeking to engage in “personally identifiable advertising,” which should be defined as “the merger of information that, by itself, can be used to identify someone — such as name, e-mail address, physical address, or telephone number — with data collected through multi-site advertising or behavioral advertising for the purposes of ad targeting.” A third party planning to use data associated with personally identifiable information for ad targeting (either online or offline) should either de-identify such data or take additional steps to notify consumers and obtain appropriate consent. More specifically:

1. Third parties should de-identify information before using it for the purpose of serving ads or connecting it with data collected through multi-site or behavioral advertising. Consumers are best served when upfront steps are taken to ensure that information that can be used to personally and directly identify them is separated from information collected through multi-site or behavioral advertising before that information is used to deliver targeted ads. Microsoft, as described in the attached white paper, applies a one-way cryptographic hash function to remove personally identifiable elements from the set of information collected from consumers and to create an anonymized identifier that it uses to serve ads online.
2. If the data is not de-identified, third parties should ensure that all privacy notices include clear descriptions of the procedure for consumers to opt out of having personally identifiable information combined with non-personally identifiable information collected on a prospective basis for ad targeting (including a description of the circumstances that would make it necessary for a consumer to renew the opt out, such as when a consumer changes computers, changes browsers, or deletes relevant cookies) and a

link to a place where consumers can exercise such choice. This includes pass-through notices, which means third parties should take reasonable efforts to require that website operators notify consumers of the procedure for opting out of having personally identifiable information merged with non-personally identifiable information collected on a prospective basis for ad targeting and a link to a place where consumers can exercise such choice.

3. Third parties should obtain affirmative opt-in consent before combining previously collected non-personally identifiable information with personally identifiable information for either online or offline ad targeting.

E. Third parties should be required to obtain affirmative express consent before using sensitive personally identifiable information for behavioral advertising.

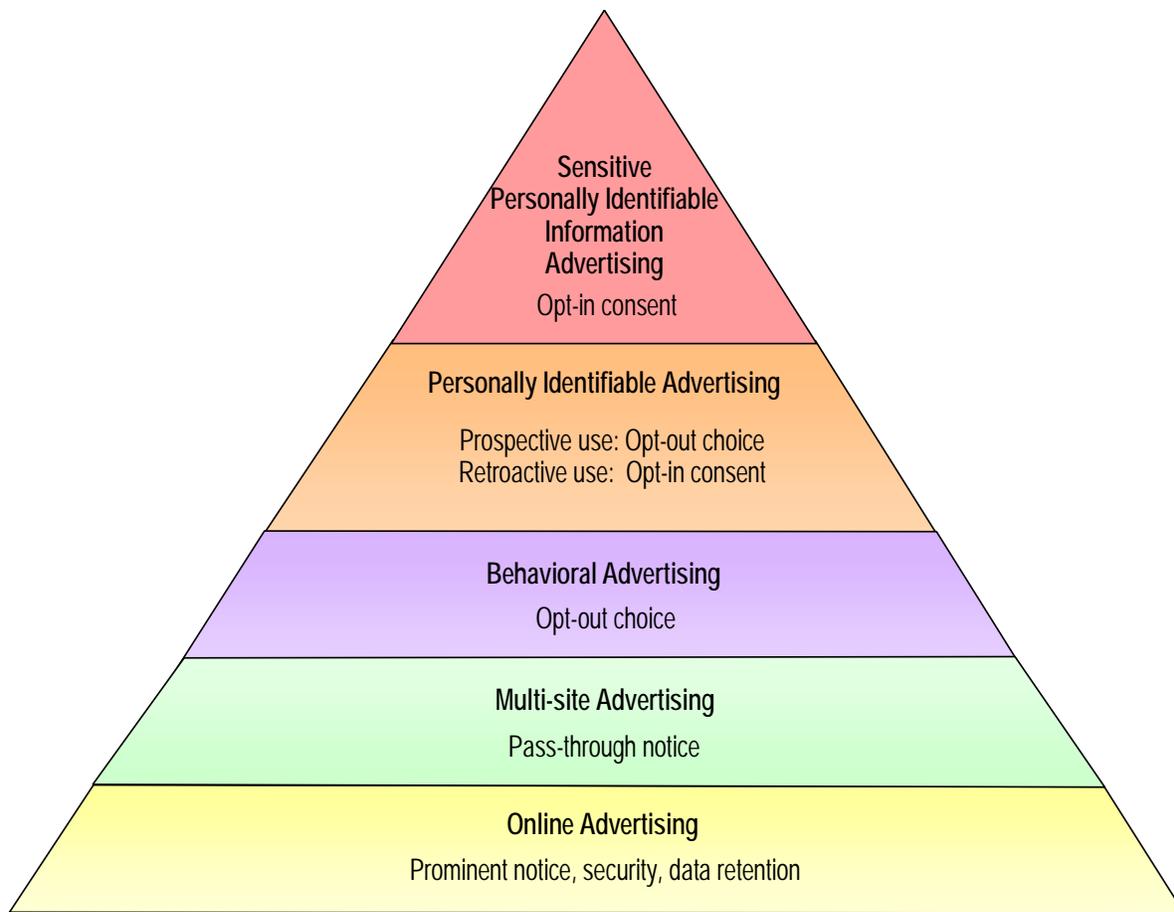
Microsoft agrees with the Commission that the use of sensitive personally identifiable information to target online ads demands heightened protection. Sensitive personally identifiable information about users — such as their health or medical conditions, sexual behavior or orientation, or religious beliefs — requires special protection. Again, privacy concerns are most pronounced when a third party uses sensitive personally identifiable information for behavioral advertising.

Microsoft therefore urges the Commission to consider a final tier for “sensitive personally identifiable information advertising”—and to define it as “the use of sensitive personally identifiable information for the purpose of behavioral advertising.”¹⁴ To address the need for greater transparency and consumer control with respect to these activities, a third party seeking to engage in sensitive personally identifiable information advertising should either de-identify sensitive personally identifiable information before using it for the purpose of serving ads, or obtain consent as follows:

1. Obtain affirmative express consent before using sensitive personally identifiable information for behavioral advertising.
2. Provide a mechanism for revoking such consent on a prospective basis.

¹⁴ We recognize that there may be concerns about the use of sensitive categories of data for behavioral advertising, whether or not the data constitutes personally identifiable information. However, for targeting activities that do not involve personally identifiable information — for example, where the entity engaged in targeting does not have a direct relationship with the individual, it may be impractical or impossible to obtain express opt-in consent. Thus, we propose an express opt-in requirement only for the use of sensitive personally identifiable information. Third parties that use sensitive non-personally identifiable information for behavioral advertising would be required to offer opt-out choice.

In short, self-regulatory principles for online advertising should be calibrated to the particular type of online advertising activity undertaken by an entity. In all instances, an entity engaged in online advertising or multi-site advertising should be required to ensure consumers receive notice about their advertising activities. As the information upon which ads are delivered becomes more personal or sensitive, additional obligations should follow. This tiered and nuanced approach appropriately recognizes the different privacy concerns posed by different forms of online advertising. It can be briefly summarized graphically as follows:



V. **REASONABLE SECURITY AND LIMITED DATA RETENTION OBLIGATIONS SHOULD APPLY TO ALL DATA COLLECTED BY ENTITIES ENGAGED IN ONLINE ADVERTISING**

Microsoft agrees with and supports the Commission’s proposed self-regulatory principles around security and data retention. These principles should apply to any entity engaged in online advertising. The proposed principles recognize that appropriate and effective security and retention practices will depend on a number of factors, and that entities should have the flexibility to adopt practices responsive to the level of risk presented.

A. Reasonable Security

Microsoft is committed to protecting the security of information we collect and maintain. We have adopted strong data security practices, implemented meaningful data protection and security plans, and undertaken detailed third-party audits. We also have taken steps to educate 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 security issues.

Microsoft's data security efforts extend to information we collect through online advertising. As described above, we have designed our systems and processes in ways that minimize the privacy impact of the data we collect and use to deliver ads online. Our online ad targeting platform selects appropriate ads based only on data that does not personally and directly identify individual users, and we store clickstream and search query data used for ad targeting separately from individually identifying account information. We also have committed to continue to implement technological and process protections to help guard the information we maintain.

The Commission's proposed self-regulatory principle around security is appropriately based on a reasonableness standard. Such an approach recognizes that security is an ongoing process, that the threats to data security are constantly changing, and that the degree and type of risk can vary from one situation to another. We agree with the factors identified by the Commission as relevant to determining whether an entity has taken reasonable security measures, including (1) the sensitivity of the data at issue, (2) the nature of a company's business operations, (3) the types of risks a company faces, and (4) the reasonable protections available to a company. This approach gives entities engaged in online advertising — which are in the optimal position to assess the particular security measures that are best suited to the different types of information they maintain — the discretion to implement the most appropriate technologies and procedures for their respective environments.

B. Limited Data Retention

Microsoft agrees with the Commission that entities that collect data through online advertising “should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.” As the Commission notes, there are often sound and legitimate business reasons for retaining data collected from users. These reasons include enhancing fraud detection efforts, helping guard consumers against security threats, understanding website usage, improving the content of online services, and tailoring features to consumer demands.

Microsoft's policy around retaining search query data provides a good example of the careful balance of interests that must be taken into account when analyzing retention periods. As noted above, Microsoft has committed to make all Live Search query data completely and irreversibly anonymous after 18 months, unless the company receives user consent for a longer time period. This policy will apply retroactively and worldwide, and will include permanently removing the entirety of the IP address and all other cross-session identifiers, such as cookie IDs and other machine identifiers, from the search terms.

Of course, the factors involved may be complex and will vary from one company to the next. For Microsoft, we believe that retaining search data for 18 months strikes an appropriate balance and, in the context of the other factors involved, provides a strong approach to protecting user privacy. Especially in light of our stringent approach to anonymization, we determined 18 months was appropriate based on the need to store some data about users to protect against security threats and improve our services.¹⁵ However, what is deemed “necessary” will differ depending on the circumstances, and flexibility is preferable to hard and fast deadlines.

VI. THE COMMISSION SHOULD CLARIFY THAT MATERIAL CHANGES MAY WARRANT DIFFERENT LEVELS OF NOTICE AND CONSENT

Microsoft recognizes the importance of privacy policies as both a tool for consumers to make informed choices about whether to interact with a business or to take advantage of a particular service offering, and as a means to promote accountability among businesses. This is true whether the privacy policy is intended to inform consumers about online advertising activities or other data handling practices. Microsoft takes all of its privacy commitments seriously and seeks to ensure consumers understand these commitments both at the outset and as our business practices change over time.

Microsoft further appreciates that material changes to privacy practices may warrant heightened forms of notice and consumer consent. That said, there appears to be some confusion around what types of changes should be considered material. In general, we believe material changes should be considered those that a consumer, acting reasonably under the circumstances, would deem important to his or her decision to visit a particular website or use a particular online service.¹⁶ For example, a website operator’s decision to start selling personally identifiable information to third parties would constitute a material change in most circumstances. There may be other changes that are less significant that, depending upon the representations previously set forth in a privacy notice, could also still be considered material to a reasonable consumer.

In light of the different types of changes that could be deemed material, we believe a nuanced approach to notice about such changes and consumer consent is warranted.

¹⁵ More specifically, because normal search behavior varies on a seasonal or annual basis, 18 months of data enables us to create a reliable baseline, which can then be used to identify various security threats, including botnet attacks, spam, click fraud, and worms. In addition, to improve the search experience for customers, it is important to have a sufficient amount of data to account for seasonal variation in search behavior.

¹⁶ The FTC’s Deception Policy Statement specifies that to determine whether a representation, omission, or practice contained in an advertisement is material, “[t]he basic question is whether the act or practice is likely to affect the consumer’s conduct or decision with regard to a product or service.” *See* FTC Policy Statement on Deception, Oct. 1983, *available at* <http://www.ftc.gov/bcp/policystmt/ad-decept.htm>. More generally, this accords with FTC guidance that, in the advertising context, materiality is to be assessed from the perspective of the consumer. *Id.*

More specifically, we urge the Commission to clarify that the following additional factors are relevant to determining the appropriate level of consumer notice and consent in a particular circumstance: (1) whether the change will be applied retroactively or prospectively, (2) the extent to which the change conflicts with a previous promise in a privacy notice, and (3) the likely significance or importance of the change (e.g., whether it involves an internal use of information within the company, or whether it involves a disclosure to a third party). The following two sections discuss the rationale behind this approach and how each factor could be applied in practice.

A. Retroactive Changes

Where a company seeks to apply a change to its privacy policy retroactively, the potential arises that it will alter promises it made at the time the data was originally collected, necessitating a heightened level of notice and choice. In those instances where a proposed retroactive change (1) is material and (2) involves a new practice that explicitly conflicts with a practice or promise set forth in the original privacy policy, the Commission has found individual notice and affirmative express (opt-in) consent to be warranted.¹⁷

In contrast, in those instances where a proposed retroactive change (1) is material but (2) does not directly conflict with a prior promise, notice and a meaningful opportunity to avoid the practice should be deemed generally sufficient. The exact level of notice and choice, however, should vary with the significance of the change. Thus, a particularly invasive practice — e.g., a company's decision to sell personal information to third parties — should necessitate individual e-mail notice to all affected consumers and require that each customer affirmatively opt in to the disclosure. A less invasive practice — e.g., a company's decision to use personal information to market its own products — should require notice to consumers with the opportunity to opt out of the new practice.

B. Prospective Changes

Where material changes are applied only to information collected following the change in policy (i.e., prospectively), there is less danger of consumer deception or other harm. Users tend to be aware that privacy policies are subject to change and typically receive notice of this potentiality in the privacy policies posted online. Accordingly, a prospective change is more likely to be anticipated by consumers. Nevertheless, some form of heightened notice alerting regular users of a service or website to a change is warranted.

Microsoft believes a nuanced, fact-specific analysis should be employed to determine the appropriate level of heightened notice for prospective privacy policy changes. For

¹⁷ Cf. Consent Order, *In the Matter of Gateway Learning*, available at <http://www.ftc.gov/os/caselist/0423047/040707agree0423047.pdf>. (finding express consent necessary to sell personal information where respondent's prior privacy policy stated that the company would neither sell, rent, or loan to third parties any personal information absent explicit consent, nor provide to any third party for any purpose any personal information about children under the age of thirteen).

example, a website operator might place a notice next to a link to the website’s amended privacy policy on its homepage, as well as a notation on the privacy policy informing the reader that the policy has been recently amended and stating the new effective date. Such notice should be sufficient to inform a reasonable consumer that a material change in the website’s privacy policy has occurred and should afford the consumer the opportunity to learn more about the details of the change.

Additional levels of notice may be warranted depending on the significance or importance of the prospective change and whether it directly contradicts an existing statement in the policy. A material change involving a highly invasive privacy practice — such as a decision to begin selling personal information — would clearly warrant additional protections. Similarly, a material and prospective change in privacy practices is more likely to defeat consumer expectations where the new policy directly contradicts the superseded policy regarding the use, collection, or disclosure of personal information. In these circumstances, a more prominent notice, such as a pop-up message or similarly visible text, may be appropriate.

VII. MICROSOFT DOES NOT USE DATA ABOUT USERS’ ONLINE ACTIVITIES FOR PURPOSES THAT RAISE PRIVACY CONCERNS

The Commission has requested additional information about the potential “secondary” uses of information gathered about users’ online activities and whether any of these uses raise concerns. We cannot speak for other companies, but as described in our privacy statement, Microsoft currently collects information to operate and improve its sites and to deliver the services or carry out the transactions our users have requested. These uses may include providing users with more effective customer service; making the sites or services easier to use by eliminating the need for users to repeatedly enter the same information; performing research and analysis aimed at improving our products, services and technologies; and displaying content and advertising that are customized to our users’ interests and preferences. The information we collect is not used for purposes outside of those disclosed to users in our privacy statement. Thus, the use of this information for these purposes should not raise additional privacy concerns that warrant notice or consent beyond those already provided.

VIII. CONCLUSION

Microsoft appreciates the opportunity to comment on the Commission’s proposed self-regulatory principles for online advertising and applauds the Commission’s focus on this important set of issues. We hope that our comments help clarify the scope and application of the principles. With these changes, the Commission’s principles provide sound guidance to online advertisers and will help ensure that consumers’ privacy interests are protected as they continue to enjoy the proliferation of free services and information that online advertising supports.

If you have any questions about our comments, please do not hesitate to let me know. Microsoft looks forward to working with you and other stakeholders to protect consumers' privacy online.

Sincerely,

/s/ Michael H. Hintze
Associate General Counsel
Microsoft Corporation

Attachments

- Privacy Protections in Microsoft's Ad Serving System and the Process of "De-identification"
- Microsoft's Privacy Principles for Live Search and Online Ad Targeting

Attachment B:
Privacy in the Cloud Computing Era

Trustworthy Computing



Privacy in the Cloud Computing Era

A Microsoft Perspective

November 2009

The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of Microsoft.

Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

© 2009 Microsoft Corp. All rights reserved.

Microsoft, Bing, Hotmail, Microsoft Dynamics, MSN, and Windows Live are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

Contents

Cloud Computing and Privacy	1
The Evolution of Cloud Computing	1
Privacy Questions in Cloud Computing.....	2
Consumer-Oriented Cloud Computing Today.....	3
Cloud Computing for Governments and Businesses	4
Legal and Regulatory Challenges.....	5
Conclusion.....	6

Cloud Computing and Privacy

A new generation of technology is transforming the world of computing. Internet-based data storage and services—also known as “cloud computing”—are rapidly emerging to complement the traditional model of software running and data being stored on desktop PCs and servers. In simple terms, cloud computing is a way to enhance computing experiences by enabling users to access software applications and data that are stored at off-site datacenters rather than on the user’s own device or PC or at an organization’s on-site datacenter.

E-mail, instant messaging, business software, and Web content management are among the many applications that may be offered via a cloud environment. Many of these applications have been offered remotely over the Internet for a number of years, which means that cloud computing might not feel markedly different from the current Web for most users. (Technical readers will rightly cite a number of distinct attributes—including scalability, flexibility, and resource pooling—as key differentiators of the cloud. These types of technical attributes will not be addressed here because they are outside the scope of this document.)

Cloud computing does raise a number of important policy questions concerning how people, organizations, and governments handle information and interactions in this environment. However, with regard to most data privacy questions as well as the perspective of typical users, cloud computing reflects the evolution of the Internet computing experiences we have long enjoyed, rather than a revolution.

Microsoft recognizes that privacy protections are essential to building the customer trust needed for cloud computing and the Internet to reach their full potential. Customers also expect their data and applications stored in the cloud to remain private and secure. While the challenges of providing security and privacy are evolving along with the cloud, the underlying principles haven’t changed—and Microsoft remains committed to those principles. We work to build secure systems and datacenters that help us protect individuals’ privacy, and we adhere to clear, responsible privacy policies in our business practices—from software development through service delivery, operation, and support.

Enterprise customers typically approach cloud computing with a predefined data management strategy, and they use that strategy as a foundation to assess whether a given service offering meets their specific needs. As a result, privacy protections might vary in different business contexts. This is not new or unique to the cloud environment. Ultimately, we expect the technology industry, consumers, and governments to agree on baseline privacy practices that span industries and countries. As that consensus view evolves, Microsoft will remain an active voice in the discussion—drawing on our extensive experience and our commitment to helping create a safer, more secure Internet that enables free expression and commerce.

The Evolution of Cloud Computing

Services that operate in the cloud often work in tandem with a client application operating on the desktop computer. For example, instant messaging and e-mail applications running on a computer rely on the cloud infrastructure for their connected features and also require a client download. The combination of “client

plus cloud” offers consumers, governments, and businesses greater choice, agility and flexibility while also greatly increasing efficiency and lowering information technology (IT) costs. It gives customers access to information, software, and services on a range of intelligent devices, at a lower cost. As a result, this next generation of computing has enormous potential to create new business opportunities and economic growth.

As with other major technological transitions, the evolution of cloud computing has drawn widespread attention and scrutiny in the news media. It has also raised policy questions concerning how people, organizations, and governments handle information and interactions in this environment. These questions are not unlike those raised during other technology-driven transitions, such as the shift from records, cassettes, and compact discs to MP3 files and from printed newspapers to online news. In these examples, the unique properties of a new medium triggered a period of adjustment that involved realigning usage practices, policies, and even regulatory approaches.

In the case of the cloud, this shift has been under way for a number of years as part of an ongoing evolution from processing information on paper and storing it in filing cabinets to storing it on computer servers outside of the user’s immediate physical control. A key distinction of cloud computing is that information storage and usage need not be limited by space or geography. Indeed, cloud computing users typically don’t even need to know how many “virtual filing boxes” they will need because the available space scales to meet their needs. Further, the cloud does far more than just store data. It also hosts applications and enables cheaper, more flexible uses of the cloud’s contents.

Privacy Questions in Cloud Computing

These properties of client-plus-cloud computing raise valid questions about security and privacy, such as:

- Are hosted data and applications within the cloud protected by suitably robust privacy policies?
- Are the cloud computing provider’s technical infrastructure, applications, and processes secure?
- Are processes in place to support appropriate action in the event of an incident that affects privacy or security?

Security is an essential component of strong privacy safeguards in all online computing environments, but security alone is not sufficient. Consumers and businesses are willing to use online computing only if they trust that their data will remain private and secure. (See the related paper titled “[Securing Microsoft’s Cloud Infrastructure](#).”¹) The ability of cloud computing providers to live up to these expectations is critical not only for the future of cloud computing but also for protecting fundamental rights of privacy and freedom of expression.

Microsoft has been examining and addressing privacy challenges in the evolving cloud computing realm for well over a decade. Our extensive experience has helped us develop well-defined business practices, privacy policies, and security measures that govern our cloud computing ecosystem. Recognizing that the cloud poses some new security and privacy challenges, we believe that our current policies and practices provide a solid foundation for addressing privacy issues and enabling greater trust in the Internet going forward.

¹ www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf

Consumer-Oriented Cloud Computing Today

Over the past decade, rapidly growing Internet-based services such as e-mail, blogging, social networking, search, and e-commerce have substantially redefined the way consumers communicate, access content, share information, and purchase products. Since the launch of the MSN® network in 1994, Microsoft has actively

Microsoft Privacy Principles

- **Accountability** in handling personal information within Microsoft and with vendors and partners
- **Notice** to individuals about how we collect, use, retain, and disclose their personal information
- **Collection** of personal information from individuals only for the purposes identified in the privacy notice we provided
- **Choice and consent** for individuals regarding how we collect, use, and disclose their personal information
- **Use and retention** of personal information in accordance with the privacy notice and consent that individuals have provided
- **Disclosure or onward** transfer of personal information to vendors and partners only for purposes that are identified in the privacy notice, and in a security-enhanced manner
- **Quality assurance** steps to ensure that personal information in our records is accurate and relevant to the purposes for which it was collected
- **Access** for individuals who want to inquire about and, when appropriate, review and update their personal information in our possession
- **Enhanced security** of personal information to help protect against unauthorized access and use
- **Monitoring and enforcement** of compliance with our privacy policies, both internally and with our vendors and partners, along with established processes to address inquiries, complaints, and disputes

addressed privacy and security considerations in its online services. Today, we manage a cloud-based infrastructure and platform for more than 200 online services and Web portals for consumers, including Windows Live™ Hotmail®, Windows Live Messenger, and Bing™ search. Because Microsoft has a direct relationship with consumers for these services, we establish and directly manage the privacy policies that govern data associated with these services.

Microsoft has long maintained that in order for individuals and organizations to fully utilize the power of computers and the Internet, the overall ecosystem must be more secure and reliable. We also believe that individuals and organizations must have greater control over their information and be able to trust that this information is being used and managed appropriately.

The foundation of Microsoft's approach to privacy and improved data protection is a commitment to empowering people to help control the collection, use, and distribution of their personal information. Microsoft was one of the first organizations to embrace the Safe Harbor privacy principles developed by the U.S. Department of Commerce and the European Commission. These tenets provided a framework for the development of Microsoft's own privacy principles, which guide our use and management of customer and partner information. (See sidebar at left.)

Together, our privacy principles and corporate privacy policy govern the collection and use of all customer and partner information and provide Microsoft employees with a clear and simple framework to help ensure privacy compliance companywide.

As a part of our Trustworthy Computing initiative, Microsoft employs more than 40 full-time privacy professionals across the company, with several hundred

more employees responsible for helping to ensure that privacy policies, procedures, and technologies are applied within the company's products, services, processes, and systems.

Further, the Microsoft Privacy Standard for Development (MPSD) framework helps ensure that customer privacy and data protections are systematically incorporated into the development and deployment of Microsoft products and services. The MPSD includes detailed guidance on creating customer notification and consent procedures, providing sufficient data security features, maintaining data integrity, offering user access, and supplying controls when developing software products and Web sites. In an effort to share best practices with the broader technology industry and privacy community, Microsoft has publicly released a version of its [Privacy Guidelines for Developing Software Products and Services](#).²

We continually review and refine the privacy policies and codes of conduct that govern our online applications in order to address consumers' evolving needs and expectations.

Cloud Computing for Governments and Businesses

Many of the same privacy policies, principles, and technologies that govern our delivery of consumer-oriented cloud computing services also apply to cloud computing for governments and businesses. Adoption of cloud computing in these sectors has accelerated as organizations have recognized its compelling potential to reduce capital and staffing costs by moving e-mail and other services into a cloud environment. Cloud-based services can also be quickly implemented and modified to meet customer demand anytime and anywhere. This allows governments and businesses to add or reduce computing capacity nearly instantaneously and pay only for the services they need. These advantages are leading organizations to put mission-critical services such as customer relationship management, enterprise resource planning, financial data management, e-mail, and document management into the cloud.

Unlike our consumer business, in which Microsoft has a direct relationship with consumers and directly controls the policies that govern their data, our cloud services for business customers defer to the policies of those customers. In this case, Microsoft has no direct relationship with the business's employees or the customers to whom the hosted data may pertain. Policies relating to the business's handling of this data in the cloud environment are controlled and set by that business rather than by Microsoft. Our role is to handle and process the data on behalf of the business, much like third-party telephone call centers process customer inquiries, orders, and data for their business customers.

The division of responsibility between an enterprise or government and its cloud services provider is similar to that of a company that rents physical warehouse space from a landlord for storing boxes of customer or company files. Even though someone else might own the building, access to those files and the use of information within them is still governed by the policies of the company that rents the space. These same principles should apply in the cloud environment.

² <http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83EC-A18D1AD2FC1F&displaylang=en>

Documents stored on an organization's own internal servers have a measure of built-in security and privacy based on the physical boundaries and access controls that the company can impose directly. As data moves into the cloud, these natural protections no longer apply in the same way. Assurance of privacy and security will require firm policies on data access, usage, and transfer that will remain in force no matter where the data travels or how it is used. Some companies will prefer to store and manage their documents and data on their own servers, while others will prefer a cloud environment or some combination of the two approaches. Microsoft offers customers all three options, which are backed by a range of security tools to help customers protect documents and data against theft, security breaches, and other types of compromise.

To prepare for the growth of cloud computing, Microsoft has developed clear and transparent data handling processes in its hosted-services agreements with enterprise customers for Microsoft Dynamics® CRM Online, Microsoft® Business Productivity Online Standard Suite, and many other services. Microsoft also provides enterprise customers with a set of flexible management tools in its enterprise platform offerings that help to protect sensitive and confidential data and support compliance with related government guidelines.

These types of transparent policies and strong protective tools are essential for enterprises as they deal with the additional privacy and security questions that arise from their use of the cloud environment to store, organize, and share data—questions that go beyond those associated with consumer-oriented cloud computing services.

Microsoft is working closely with its enterprise customers to help address these considerations through well-defined policies governing cloud-based management, use, and protection of data. This includes making sure that as enterprises increasingly move from storing data in-house to contracting with cloud-services providers for hosted management, clear privacy guidelines define what the provider can and cannot do with data it is safeguarding.

Legal and Regulatory Challenges

Cloud services can thrive when companies are able to provide these services in an efficient way and assure customers that their data will remain private and secure. But as more and more consumer and enterprise data moves into the cloud, increasing uncertainty about the legal and regulatory obligations related to that data could jeopardize the benefits of cloud computing.

To offer the full benefits of cloud computing, online computing providers must be able to operate datacenters in multiple locations and transfer data freely between them. This allows a provider to optimize efficiency and deliver the performance and reliability that customers expect. Regulations that restrict cross-border data transfers, or create uncertainty or disharmony with respect to such transfers, can hamper these benefits.

Similarly, providers can be caught in an impossible position when governments impose conflicting legal obligations and assert competing claims of jurisdiction over user data held by these providers. Divergent rules on data privacy, data retention, law enforcement access to user data, and other issues can lead to ambiguity and significant legal challenges. For instance, one country might insist that its rules regarding mandatory data retention or law enforcement access to data apply in a given context. However, this could result in a situation

where there is a direct conflict with the privacy laws of another country that also has a strong claim of jurisdiction over that same data.

While IT companies will face the brunt of these problems first, their effects will increasingly be felt across the economy. If businesses are forced to store data locally in order to mitigate these jurisdictional conflicts, the costs of investment and innovation in cloud computing will increase. As a result, many of the efficiency and performance benefits of cloud computing may be lost and the benefits to business and consumers will be reduced.

The IT industry has been working hard to address these challenges, but it cannot solve them alone. Microsoft supports efforts to develop globally consistent privacy frameworks that recognize the worldwide nature of data flows while at the same time providing strong privacy protections for the people to whom the data pertains. More generally, governments must help craft clear rules and processes to resolve these conflicting obligations in a way that protects privacy and security.

Conclusion

Client-plus-cloud computing offers enhanced choice, flexibility, operational efficiency and cost savings for businesses and consumers. To take full advantage of these benefits, users must be given reliable assurances regarding the privacy and security of their online data. In addition, a number of regulatory, jurisdictional, and public policy issues remain to be solved in order for online computing to thrive.

Microsoft has been addressing many of these issues since 1994, when we delivered our first online services for consumers and enterprises. Our breadth of experience has shaped our company's privacy principles, corporate privacy policy, product and service development, and overall business practices. These components anchor our commitment to maintaining the highest standards of privacy and security in our online services and to partnering with other industry leaders, governments, and consumer organizations to develop globally consistent privacy frameworks that enable the expansion of the economic and social value of cloud-based computing.

**Attachment C:
Written Testimony of Michael Stokes
Before the Senate Judiciary Committee**

**Written Testimony of
Michael Stokes
Principal Program Manager, Microsoft Corporation's Health Solutions Group**

**Before the
Senate Judiciary Committee**

Hearing on Health IT: Protecting Americans' Privacy in the Digital Age

January 27, 2009

Chairman Leahy, Ranking Member Specter, and distinguished members of the Committee, my name is Michael Stokes, and I am a Principal Program Manager in Microsoft's Health Solutions Group. In this role, I focus on privacy issues, and I very much appreciate the opportunity to share Microsoft's views on the importance of privacy and health IT. We commend the Committee for holding this hearing today and for your efforts at the intersection of privacy, information technology, and healthcare reform. We are committed to working collaboratively with you, the Department of Health and Human Services, the Federal Trade Commission, consumer advocates, and other stakeholders to protect the privacy of health data.

Microsoft is here today because we are deeply engaged on both health IT and privacy issues. Over 12 years ago, Microsoft began developing technologies focused on the health industry, with the goal of using software and the Internet to transform healthcare, as they have so many other industries—opening new ways of working, new ways of communicating, and new economics. Our products, including HealthVault for consumers and Amalga for hospitals and health systems, are focused on driving scalable health IT solutions that can benefit all.

Microsoft also has a deep and long-standing commitment to privacy. We recognize that consumers will only be comfortable sharing their information if they trust that they will have control over its use and know that it will be protected. Establishing trust is especially important with respect to health data. This is because of the important role that health data plays in our overall healthcare system. Delivering quality, reliable healthcare requires that data be shared. New therapies, new cures, and new lessons about disease will be driven by the availability of health data. By working together to encourage data liquidity through strong privacy protections, we can realize the value of data sharing and thereby drive real change in our healthcare system.

Today, I want to discuss how we can promote the widespread use of innovative health IT solutions and the sharing of health data while still protecting privacy. My testimony today begins by describing what we believe to be the future of healthcare—a totally connected environment where patients and providers trust each other and use health IT to share information seamlessly. It then discusses how the three components of trust—transparency, control, and security—can provide flexible technology solutions that improve our current healthcare system. It concludes by showing how the same principles of transparency, control, and security underlie Microsoft's approach to privacy in health IT.

I. The Future: Dynamic, Trusted, Consumer-Driven Healthcare

There has been much discussion and debate about how to improve the healthcare system in the United States. But we think it is fair to say that we all have a single goal in mind: to deliver predictive,

preventive, and personalized medicine in an accessible, affordable, and accountable way. In our view, health IT and privacy are necessary elements to achieve this success.

A. Health IT Can Build a Patient-Centric System

The future of medicine and improvements in our healthcare system depend on the seamless exchange and reuse of health data. Today, in order to manage their health, consumers must deal with both paper documents and electronic files. Few people have the resources to keep track of medication lists, vaccination histories, appointment calendars, lab results, diet plans, exercise schedules, and all the other components of health data. Most people have little knowledge of how to prevent disease and little, if any, support for managing their healthcare.

What if consumers could collect all their health and wellness data electronically, could keep it securely stored in one place over time, and could share relevant elements of this record securely from provider to provider, no matter the doctor or insurance company with whom they interact? With all the relevant data at their fingertips, accessible at any time and any place, they could sign up for services that provide personalized alerts and information. They could track fitness goals across numerous devices, such as exercise bikes that monitor vital signs, smart watches that record the number of miles run, and scales that measure body fat as well as weight. They could research relevant medical conditions online and interact with support groups so that they would be better prepared and informed for their next visit to the doctor. And they could share data with their support systems and make better health decisions for themselves and their families.

A patient-centric system would benefit healthcare professionals and hospitals as well. Today, patients often see multiple doctors, often spread across multiple health systems. Each doctor sees only a fragment of the patient's health data, which can lead to unsound medical decisions and excessive costs. Health IT can connect an individual's existing data, allowing healthcare professionals to see a complete picture of their patient. This will enable providers to eliminate unnecessary procedures, avoid harmful drug interactions, and concentrate on providing better quality care.

At Microsoft, we believe technology can make this vision a reality without sacrificing privacy protections. We envision a healthcare ecosystem that places patients at the center of a protected and connected network, with:

- Patients as consumers—experiencing more control, more convenience, better service, and ultimately better value for what they spend on healthcare.
- Physicians as knowledge workers—professionals getting the right data in the right format at the right time to provide the best treatment and preventive care.
- New interactions among the key members of the healthcare ecosystem—physicians, patients, pharmacies, researchers, and insurance providers benefiting from a new flow of data to make better, faster decisions.
- The extension of modern healthcare to the virtual space—patients getting care when they want it, wherever they need it, thanks to virtual medical clinics, virtual doctor visits, virtual lab results, medical homes, and personalized medicine based upon genomic data.

- A learning healthcare system—one that measures key data points, identifies errors, and makes improvements in order to deliver value.

In this new healthcare system, everyone will have the right information at the right time with computer-assisted decision support, enabling the seamless exchange and reuse of data. Health data is the asset that will drive an efficient, high-quality, value-based, evidence-focused future for medicine, achieving one of the priorities of Congress and the new Administration.

B. Trust Is Essential to a Patient-Centric Healthcare System

Health data is the fuel that will drive a connected, patient-centric healthcare system. It is therefore critical that consumers, providers, and other participants in the healthcare ecosystem be willing to share health data. To facilitate such sharing, we must establish a foundation of trust.

Health data is often considered more sensitive than other personally identifiable information. If health data is stolen or lost, it is not simply a matter of recovering financial assets. It can impact an individual's employment, ability to receive healthcare, and social standing. And the effects are not limited to the individual whose data was lost, because health data may also be relevant to the person's children, grandchildren, or distant relatives. Indeed, there is evidence that many Americans do not actively participate in their own healthcare due to privacy concerns:

- According to the Department of Health and Human Services, two million Americans with mental illness do not seek treatment for this reason.¹
- Approximately 600,000 cancer victims do not seek early diagnosis and treatment.²
- Millions of young Americans suffering from sexually transmitted diseases do not seek diagnosis and treatment (1 in 4 teen girls are now infected with an STD).³
- The California HealthCare Foundation found that 1 in 8 Americans have put their health at risk by engaging in privacy-protective behavior: avoiding their regular doctor, asking a doctor to alter a diagnosis, paying privately for a test, or avoiding tests altogether.⁴
- The Rand Corporation estimated that 150,000 soldiers may be suffering from Post-Traumatic Stress Disorder (PTSD), many of whom do not seek treatment because of privacy concerns.⁵

¹ Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,779 (Dec. 28, 2000).

² *Id.* at 82,777.

³ *Id.* at 82,778; Press Release, Centers for Disease Control and Prevention, Nationally Representative CDC Study Finds 1 in 4 Teenage Girls Has a Sexually Transmitted Disease (Mar. 11, 2008), <http://www.cdc.gov/STDConference/2008/media/release-11march2008.htm>.

⁴ California HealthCare Foundation, *National Consumer Health Privacy Survey 2005* (Nov. 2005), <http://www.chcf.org/topics/view.cfm?itemID=115694>.

⁵ RAND Corp., *Invisible Wounds of War* 55, 104, 436 (2008), <http://www.rand.org/pubs/monographs/MG720/>.

Because health data can be highly sensitive, consumers and healthcare providers will only share such data if they trust that the privacy of health data will be protected. When such trust is established, data will flow freely, benefiting all participants. Consumers will receive better information about appropriate treatments, medications, nutrition, and exercise. Healthcare providers will receive more reliable health data and greater patient compliance, which in turn leads to better quality care and improved cost efficiencies both for treatment of individual patients and for public health purposes. In short, effective privacy protections are critical to the success of health IT and healthcare in general.

II. Trust Requires Transparency, Control, and Security

Transparency, control, and security are necessary to help ensure that consumers and healthcare providers trust, and are willing to participate in, the healthcare system.

A. Transparency Can Help Stakeholders Understand How Their Data Is Used

Transparency is significant because it provides consumers with an informed understanding of a company's data collection practices, of how their data might be used, and the privacy controls available to users. Without transparency, consumers are unable to evaluate a company's services, to compare the privacy practices of different entities to determine which products and services they should use, or to exercise the privacy controls that may be available to them. Transparency also helps ensure that when consumers are dealing with a company that has adopted responsible privacy practices, consumers do not needlessly worry about unfounded privacy concerns that might prevent them from taking advantage of new technologies.

Transparency is especially important with respect to healthcare data. If patients do not understand what data is being collected, who has access to the data, and what the data will be used for, they may decide not to provide the information at all—not even to their treating physicians. Without this data, doctors will not be able to make fully informed treatment recommendations, and overall consumer health could suffer.

Providers need transparency too. They need to understand how the health data they make available to patients and others may be used; they need to know whether such data may be disclosed to third parties; and they need to feel comfortable that health data will be protected.

Transparency is also essential to ensure accountability. Regulators, advocates, journalists, and others have an important role in helping to ensure that appropriate privacy practices are being followed. But they can only examine, evaluate, and compare practices across the industry if companies are transparent about the data they collect and how they use and protect it.

B. Control Can Help Stakeholders Manage Their Data Effectively

Transparency by itself is not enough. Stakeholders also need control over where their data is, who is looking at it, and for what purpose. For example, control allows patients to decide when and under what conditions they want to receive alert services or medical information that might be relevant to them. And if providers can control where health data is going, they will be better able to comply with applicable laws, regulations, and policies.

Control is particularly important when the consumer or provider needs a proxy to guide his or her choices. Patients often need to share data with custodians, guardians, or family members, but they may

want to ensure that the data is only shared under certain conditions (e.g., only when the patient is unable to make decisions for himself) or only for certain periods of time (e.g., only data about the past year rather than the patient's entire lifetime). Similarly, physicians often rely on nurses, staff, specialists, and laboratory technicians to provide care for a patient. Access controls can help ensure that the patient's health data is shared only with the healthcare professionals who need to see it, and that the patient's data is not inadvertently misplaced or deleted.

At the same time, however, control should not impede the flow of clinical data that healthcare professionals need to provide effective care. For example, some members of the healthcare community have pointed out that a system requiring repeated patient consents for the disclosure of clinical data could potentially hamper treatment in situations where care must be coordinated among multiple physicians. We all need to work together to create an environment that facilitates rather than hinders care.

C. Security Can Give Stakeholders the Confidence to Adopt Health IT Innovations

Concerns about the collection and use of personal data, widely publicized security and data breaches, and growing alarm about healthcare fraud and identity theft threaten to erode public confidence in digital health solutions. Cybercriminals are increasingly exploiting personal data to make a profit, and there are a growing number of security attacks that target personal data. A recent report from the Department of Health and Human Services noted that medical identity theft can lead to patients receiving the wrong care because of inaccurate data on their health records, being blocked from receiving health insurance or other benefits, or incurring financial obligations for services that were never provided.⁶

Security helps ensure that patients and providers do not spend time and resources dealing with data breaches, identity theft, and security flaws. Once stakeholders feel confident that their data is secure, they will be more willing to adopt the innovative health IT solutions that can improve care and reduce costs. Moreover, health IT can also improve security. For example, technology that verifies patients' identities, monitors access to health records, and identifies anomalies in services requested could help prevent and detect medical identity theft.⁷

D. Transparency, Control, and Security Provide Flexible Privacy Protections

Privacy protections are not just about patients. Doctors have data of their own that they want to keep private. Additionally, hospitals, insurance plans, research facilities, and other healthcare organizations are major businesses that need to protect their intellectual property and trade secrets. Transparency,

⁶ Booz Allen Hamilton & Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, *Medical Identity Theft Final Report* (2009), <http://www.hhs.gov/healthit/documents/MedIdTheftReport011509.pdf>.

⁷ *Id.* at 14 (noting, for example, that IT systems can “review transactional records and detect such anomalies as the appearance of treatments for chronic conditions not previously diagnosed; increases in prescriptions that may indicate drug-seeking behavior; or attempts to receive care at multiple locations, all remote from the individuals’ residences”).

control, and security protect privacy in ways that are flexible enough to accommodate all stakeholders in the healthcare system, not just consumers.

Moreover, today's healthcare ecosystem consists of a complex mixture of legacy and new, innovative solutions. Retrofitting existing systems may require significant design changes, and it may not be viable for everyone to upgrade their technology systems. One potential path forward is to provide a combination of simpler, less flexible, baseline solutions and newer, more complex, extensible technologies that encourage migration toward a more privacy-protective future. Following the principles of transparency, control, and security enables participants to provide privacy protections that are flexible and vibrant enough to support all of these technical solutions and business models.

III. Microsoft's Efforts to Build Trust Through Transparency, Control, and Security

Microsoft or anyone that provides tools and technologies involving healthcare data must adopt strong privacy practices that support trust. If people feel that the privacy of their healthcare data is not being protected, they will make less use of healthcare information technologies, which can hurt them and the healthcare industry alike.

Microsoft has been deeply engaged on privacy issues. Microsoft was one of the first companies to appoint a chief privacy officer, an action we took nearly a decade ago, and there are now several hundred employees throughout the company who focus on privacy as part of their jobs. We have a strong set of internal policies and standards that guide how we do business and how we design our products and services in a way that respects and helps protect user privacy. And we have made significant investments in privacy training and in building our privacy standards into our product development and other business processes.

A. Transparency by Providing Clear Disclosures

Microsoft is committed to providing transparency in its products and services. One example is HealthVault, Microsoft's free Internet-based platform that allows consumers to store copies of their health records, upload data from home health devices, share data with healthcare providers, and access products and services to help improve their health. HealthVault's privacy statement is designed to be easy to understand. We have eliminated passive language, and we wrote the statement at a high-school reading level. We also organized the privacy statement in terms of a consumer's perspective on how to use the HealthVault service, much like an abbreviated help document. We use third-party seals such as TRUSTe and eHon, we ask advocates and regulators to review our policy before launches and major revisions, and we encourage users to provide feedback.

Moreover, the HealthVault network currently has 40 live applications—programs that can connect with HealthVault, such as personal health records and alert services. Some of these applications are provided by Microsoft's partners. Before any application is authorized to access a consumer's data, we make sure that the consumer knows which application is requesting the data, what data is being requested, what the data will be used for, and which data elements are required or optional. HealthVault also stores audit trails, so that consumers can see who has accessed their health records and what actions have been taken.

B. Control by Offering Granular Access

Microsoft has made user control a key component of our healthcare solutions. We provide many different tools to help users control how their data is accessed and used. For example, in HealthVault, consumers can control what type of data is shared, who else has access to that data, whether others are allowed to modify or only to view the data, and how long others can access the data. These tools give consumers the flexibility to adjust their access decisions as their health needs change, so that a consumer who is suddenly diagnosed with a serious condition can immediately start sharing relevant data with his treating physician. Moreover, consumers can designate other "custodians" who can then share access with others, enabling records to be transferred from parent to child as the child reaches maturity or from elderly parent to adult children for extended care.

We have also implemented control features in our other health IT products. For example, just under a year ago, we launched Amalga, our family of enterprise data sharing and intelligence solutions, which connect a hospital's or health system's existing legacy systems and any new systems. This allows patient data to be viewed and queried holistically, enabling a shift from departmentally focused systems to more patient-centric systems. Amalga includes controls that allow hospitals and health systems to determine which data is shared when and with whom.

C. Security by Following Comprehensive Best Practices

Security has been fundamental at Microsoft for many years as part of our Trustworthy Computing initiative, and we have taken a broad approach to protecting the security of personal information. This approach includes implementing technological and procedural protections to help safeguard the information we maintain. For example, Microsoft has developed a Security Development Lifecycle program that calls for security evaluations and an appropriate combination of security measures, such as independent security penetration testing, independent certifications including ISO 27001, information segmentation, Lightweight Directory Access Protocol (LDAP) integration, auditing and logging capabilities, controlled-access facilities, and encrypted Internet protocols when communicating personal health data. We also have taken steps to educate customers about ways to protect themselves, and we have worked closely with industry and law enforcement around the world to identify security threats, share best practices, and improve our coordinated response to security issues.

IV. Conclusion

Microsoft recognizes that technology is only a part of a comprehensive approach needed to drive real change in our healthcare system. Education, leadership in healthcare organizations, and meaningful public policy are also critical components to success. We look forward to partnering with you and all participants in the healthcare ecosystem to move toward dynamic, trusted, and consumer-driven healthcare. Thank you for giving us the opportunity to testify today.