MIKE HINTZE
ASSOCIATE GENERAL COUNSEL
MICROSOFT CORPORATION

SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE
COMMITTEE ON ENERGY & COMMERCE
U.S. HOUSE OF REPRESENTATIVES

SUMMARY OF TESTIMONY
HEARING ON "UNDERSTANDING CONSUMER ATTITUDES ABOUT PRIVACY"
OCTOBER 13, 2011

Microsoft engages with consumers in multiple contexts — as a website publisher, an operator of an ad network, a provider of cloud computing and other online services, and as a developer of PC and mobile operating systems, a leading web browser and other software applications — and therefore offers a unique perspective on the privacy discussion.

There is no single, "silver bullet" solution to privacy, principally because privacy means different things to different consumers; depends on the context in which data is collected and used; and is subject to a rapid pace of change in technology. Consumer sensitivities and expectations regarding privacy therefore are evolving constantly.

This necessitates a multi-factored approach to addressing consumer privacy that includes: (1) company best practices, such as privacy by design, transparency, and security; (2) technology tools, such as the browser-based "Do Not Track" mechanism that we incorporated into Internet Explorer 9 to allow consumers to make informed privacy choices for themselves; (3) industry self-regulation, such as the Self-Regulatory Program for Online Behavioral Advertising, which employs a universally-recognizable "Advertising Option" icon that consumers can access to learn about and opt out of online ads; and (4) consumer education, which equips consumers to make choices that align to their own privacy needs and helps protect them from harm.

In Microsoft's experience, consumers are using the privacy tools and information we make available to make informed privacy choices for themselves. For example:

- Over the past five months, key privacy websites offered by just one division of our company averaged over two million sessions per month.
- In an average month, more than 435,000 consumers access our "Advertisement Choice" webpage, which is the website that explains how a user can opt-out of personalized online advertisements and provides information about how and why

such advertisements are delivered. Approximately 20 percent of those consumers perform some action while visiting that web page, in most cases opting out of personalized ads.

- In an average month, approximately 16,000 U.S. consumers visit their Personal Data Dashboards, which provide a centralized location for consumers to view and manage their online information. In August 2011 alone, these visits increased to more than 22,000.

STATEMENT OF MIKE HINTZE
ASSOCIATE GENERAL COUNSEL
MICROSOFT CORPORATION

BEFORE THE
SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE
COMMITTEE ON ENERGY & COMMERCE
U.S. HOUSE OF REPRESENTATIVES

HEARING ON "UNDERSTANDING CONSUMER ATTITUDES ABOUT PRIVACY"

OCTOBER 13, 2011

Chairman Bono Mack, Ranking Member Butterfield, and honorable members of the Committee, my name is Mike Hintze, and I am an Associate General Counsel of Microsoft Corporation. Thank you for the opportunity to share Microsoft's perspective on the important issue of consumer privacy. We appreciate the leadership that the Subcommittee has shown on privacy issues, and we are committed to working collaboratively with you, the Federal Trade Commission ("FTC"), the Department of Commerce, consumer groups, and other stakeholders on ways to protect consumer privacy while promoting innovation. The multiple contexts in which we engage with consumers gives us a unique perspective on the privacy discussion. As a website publisher, an operator of an ad network, a provider of cloud computing and other online services, and as a developer of PC and mobile operating systems, a leading web browser and other software applications, Microsoft has a deep understanding of the roles that different participants play in the digital ecosystem and in safeguarding consumer privacy.

Microsoft embraces a commitment to consumer privacy because we recognize that consumer trust is critical to the adoption of online and cloud computing services that Microsoft and others in our industry offer. Our goal at Microsoft is to build trust with consumers by providing them with information about what data is being collected and how it is being used, choices about the collection and use of that data, and confidence that their data is secure. As I will describe in greater detail in my remarks, these three principles — transparency, control, and security — underpin Microsoft's approach to privacy. They are essential components of the privacy frameworks advanced by the FTC and the Department of Commerce, and we believe they represent what users have come to expect from their online experience.[1]

---

[1] *See generally* Fed. Trade Comm'n, Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010) ("FTC Staff Report"); Internet Policy Task Force, Dep't of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010).

In our experience, there is no single, "silver bullet" solution to privacy. There are several reasons for this conclusion. First, privacy means different things to different consumers, and research has shown that there is a wide range of privacy sensitivities among individuals.[2] Second, we believe that consumers often have different privacy expectations depending on the context in which their data is collected and used; for example, their expectations can differ when they interact with retailers, social media platforms, online games, search engines, or Internet service providers. To meet these differing needs and expectations, Microsoft strives to offer meaningful privacy choices in its service offerings, recognizing that informed consumers will make personal privacy choices and adopt a wide range of privacy preferences.

The challenges of crafting effective privacy solutions also are rendered complex by the rapid pace of change in technology, business models, and consumer adoption rates for online services. Within this rapidly evolving environment, user sensitivities and expectations regarding privacy also can evolve over time in particular contexts. Not too long ago, few consumers were sharing their personal photographs and home videos publicly; today, consumers regularly post these and other materials on social networking and online video websites without hesitation because they find value in these services.

---

[2] For instance, Alan Westin, a well-known privacy researcher, has concluded that individuals can be segmented into three separate groups based on their attitudes toward privacy: privacy fundamentalists, privacy pragmatists, and privacy unconcerned. *See What Consumers Have To Say About Information Privacy: Hearing before the House Subcommittee on Commerce, Trade, and Consumer Protection*, 107th Cong. 15-16 (2001) (testimony of Alan K. Westin, Professor Emeritus, Columbia University). According to Professor Westin, at one end of the spectrum, some consumers are privacy fundamentalists, meaning they are "intensely concerned about privacy" and "generally will reject benefits offered to them by a business." At the other end of the spectrum are consumers that are "privacy unconcerned," who "[don't] know what the 'privacy fuss' is all about" and "[have] little problem with supplying their personal information to government authorities or businesses." *Id.* The majority of consumers fall into the "privacy pragmatist" category; they "weigh[] the value to them and society of various business or government programs calling for personal information, examines the relevance and social propriety of the information sought, look[] to see whether fair information practices are being widely enough observed, and then decide[] whether they will agree or disagree with specific information activities." *Id.*

These challenges necessitate a multi-factored approach to addressing consumer expectations about privacy that includes (1) company best practices, (2) technology tools, (3) rules of the road established through both industry self-regulation and legislation, and (4) consumer education. Today, I will describe the steps Microsoft has taken and continues to take to protect privacy and advance these objectives. These steps demonstrate Microsoft's deep commitment to privacy, particularly in its own product design, and highlight the important role that company best practices and technology play in addressing consumer privacy and meeting consumer expectations. They also help highlight the importance of fostering an environment that will lead to appropriate privacy protections without impeding innovation. It is important to acknowledge at the outset, however, that no one company alone can fulfill all of these objectives. Addressing consumer privacy expectations often requires the collaborative effort of individual companies, industry groups, consumer and privacy advocates, government, and consumers themselves.

I. Microsoft's Commitment to Privacy in Product Design and Business Practices

Individual companies play an important role in protecting consumer privacy. At Microsoft, we have a deep and long-standing commitment to our privacy by design approach. It defines not only how we build products, but also how we design and operate our services and how we conduct our business. Microsoft was one of the first companies to appoint a chief privacy officer, an action we took over a decade ago, and we currently employ over 40 employees who focus on privacy full time and another 400 employees who focus on privacy as part of their jobs. In addition, we have adopted robust policies and standards to ensure that we do business and design our products and services in a way that respects and protects consumer privacy. For years, we have built privacy standards and checkpoints into our product development processes. Doing so helps us ensure that we engineer privacy into our products and online services at the earliest stages of their development and foster the continued consideration of privacy throughout the product lifecycle, including after the release of the product or

service into the market. We have continued to refine and develop these standards and processes over time. We have even made some of these standards available publicly to help others in the online industry adopt high standards for privacy.[3]

Microsoft also has been a leader and innovator in increased transparency by, for example, developing and being one of the first companies to adopt "layered" privacy notices. The Microsoft Online Privacy Statement provides consumers with the most important information about our privacy practices in a concise, one-page upfront summary with links to additional layers that describe in more detail our data collection and use practices.[4] We also provide information about our privacy practices and access to user controls on dedicated web pages and know that consumers are viewing this information. For example, over the past five months, key privacy websites offered by just one division of our company averaged over two million sessions per month.[5]

Microsoft's online advertising business provides illustrative examples of how we also provide consumers with meaningful choices about how their information is used. Several years ago, Microsoft decided to address a weakness inherent in offering consumers the ability to "opt out" of behavioral advertising solely via an "opt-out cookie." At the time, opt-out choices not only were wiped

---

[3] For example, Microsoft's Privacy Guidelines for Developing Software Products and Services, which are based on our internal privacy standards, are posted publicly at http://www.microsoft.com/privacy. We make these standards publicly available for other organizations to use to develop and guide their own product development processes. And our privacy guidelines are recognized by the International Association of Privacy Professional's privacy certification program – the Certified Information Privacy Professional for IT (CIPP/IT). *See* https://www.privacyassociation.org/images/uploads/CIPP_IT_Reading_List_0909.pdf.

[4] *See* http://privacy.microsoft.com/en-us/default.mspx.

[5] These key privacy websites include choice.live.com, where consumers can learn more about the online advertising process, opt out of personalized ads, and access their personal data dashboard (provided at Appendix 1); the "Advertisement Choice" website, which contains information about personalized advertising and provides an opt out option (provided at Appendix 2); and the Personal Data Dashboard website, which provides access to all of these key privacy controls in a centralized location (provided at Appendix 3). In August 2011, traffic to these privacy websites totaled 2,405,702 sessions, or approximately 1 million distinct users.

clean each time a user deleted the cookies for his or her machine,[6] but the opt-out cookies also were computer specific. To address these limitations, Microsoft began offering users the ability to tie their opt-out choices to their Windows Live ID — the credentialing protocol that consumers use to sign in to our online services. As a consequence, if a user today deletes the cookies on his or her machine, when the user signs back in with his or her Windows Live ID, that opt-out selection will persist. It also means that a user's opt-out choices can apply across multiple computers (*e.g.*, home and work computers) when the user signs in on them.

As an alternative to opting out, we also allow users to influence the ads they see by signing in through their Windows Live ID and selecting their interests. This means that users will be more likely to see ads over time that reflect their own preferences. In an average month, more than 435,000 consumers access our "Advertisement Choice" webpage, which is the website that explains how a user can opt out of personalized online advertisements and provides information about how and why such advertisements are delivered.[7] Approximately 20 percent of users that access this web page (and similar Microsoft web pages) perform some action while visiting them, in most cases opting out of personalized ads. In an average month, approximately 16,000 U.S. consumers also visit their Personal Data Dashboards, which is a new feature that we have developed to provide a centralized location for consumers to view and manage their online information. In August 2011 alone, these visits increased to more than 22,000. These company-specific efforts are, of course, in addition to the joint efforts we have undertaken with other stakeholders in the online advertising industry, which I describe in greater detail below.

---

[6] Relying solely on a cookie to store the opt-out choice was in tension with the common advice to consumers that one way to help protect privacy was to periodically clear their cookies. The result was that when a consumer cleared his or her cookies, the opt-out choice also would disappear.

[7] *See* http://choice.live.com/Default.aspx.

In short, by building transparency, choice, and security into its products from the earliest stages of design, Microsoft fosters consumer trust in its products and in the online environment and empowers users to control their personal information and make appropriate privacy choices for themselves.

II. Microsoft's Development of Technology Tools

As a technology company, we naturally believe that technology has a key role to play in protecting privacy, particularly with respect to providing consumers with a variety of choices and tools to help put them in control as they interact with sites and services across the Internet. In our capacity as a browser vendor, for example, Microsoft has developed and supported a number of innovative tools that give consumers greater control over the collection and use of information about their online actions. For example, with Internet Explorer 8, we introduced InPrivate Browsing, a feature that prevents a consumer's browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser after the consumer closes the InPrivate Browsing window.[8] This helps consumers keep their browsing history private on shared computers such as at home, in an Internet café, or at a public kiosk. Another feature introduced in Internet Explorer 8, InPrivate Filtering, analyzes third-party content and provides users with options to block third-party content providers from collecting information about users' browsing activities.[9]

Microsoft also was the first of the major browser manufacturers to respond to the FTC's recent call for a persistent, browser-based "Do Not Track" mechanism.[10] Specifically, Internet Explorer 9 offers an innovative new feature, "Tracking Protection," that allows consumers to decide which third-party sites can receive their data and filters content from third-party sites identified as potential privacy threats. When a consumer visits a website, his or her computer automatically shares information with

[8] *See* http://windows.microsoft.com/en-US/windows-vista/What-is-InPrivate-Browsing.

[9] *See* http://windows.microsoft.com/en-US/Windows7/InPrivate-frequently-asked-questions.

[10] *See* FTC Staff Report at 66.

that website, such as cookies, IP address, and other standard computer information. If the website contains content provided by a third-party website (for example, a map, advertisement, or any web measurement tools, such as a web beacon or scripts), some information about the consumer may be sent automatically to the third-party content provider.[11] Users who activate the Tracking Protection feature can create or download Tracking Protection Lists that identify third-party websites or content that are, in the view of the list creator, trustworthy or untrustworthy.[12] If a third party site is listed as a "do not track" site on a Tracking Protection List, Internet Explorer 9 will block the websites a consumer visits from making "calls" to that third party site.[13] By limiting calls to third-party websites, Internet Explorer 9 blocks these third-party sites from collecting information from users – without relying on these third-party sites to read, interpret, and honor a do-not-track signal.[14]

The Tracking Protection feature is highly customizable and can be adapted to specific user preferences because anyone on the Web (including consumer groups and privacy advocates and security firms) can create and publish Tracking Protection Lists – they simply are files that can be uploaded to a website and made available to others via a link. Consumers can create or subscribe to a list or lists as they see fit.

III. Microsoft's Support for Baseline Rules of the Road

In addition to company-specific efforts, Microsoft believes that there is need for baseline rules of the road. These rules may best be established by a combination of federal privacy

---

[11] This type of arrangement can have several benefits. For example, it enables consumers to access third-party content conveniently, and the presence of advertising may make it possible for the website to provide access to premium content at no charge. There can, however, be an impact to consumer privacy as a result because it is possible for the content providers to track individual consumers across multiple websites.

[12] *See* http://www.iegallery.com/en/trackingprotectionlists/.

[13] Information can be sent to a site listed as "do not track" on a Tracking Protection list if the user chooses to visit that site directly by clicking on a link or typing its web address.

[14] As an additional measure, if the user has installed a Tracking Protection List, Internet Explorer 9 will send a do-not-track signal or preference to all the websites the user visits.

legislation that establishes baseline principles (discussed below) and industry self-regulation that would build on those basic principles to create effective privacy protections that take into account consumers' reasonable expectations of privacy in different contexts. Industry self-regulation can and should establish minimum standards and best practices across an industry, and foster industry-wide privacy solutions. As I mentioned at the outset, consumers can have different privacy expectations depending on whether they are interacting with retailers, application developers, social media platforms, online games, search engines, Internet service providers, publishers, advertisers, or ad networks, and industry self-regulation can offer flexible tools for addressing privacy issues in these many different contexts. In addition, self-regulatory efforts are generally better able than prescriptive legislation to keep pace with evolving technologies and business models.

Microsoft has a history of working collaboratively with other companies to develop and support appropriate solutions that build on the principles of transparency, control, and security. For example, Microsoft is a strong supporter of, and is implementing, the Self-Regulatory Program for Online Behavioral Advertising, which includes the prominent display of text or a universally-recognizable "Advertising Option" icon in or next to online ads.[15] By clicking on the text or icon, consumers can easily access and learn about online behavioral advertising and the privacy practices associated with online advertising, and, with a single click, consumers can choose to opt out of receiving tailored advertising from all participating companies, if they choose. This program, which facilitates both transparency and consumer choice, also includes an educational website where consumers can learn about online advertising and choose not to have their information used for behavioral advertising.[16]

Data security also is among the focal points of the Self-Regulatory Program for Online Behavioral Advertising: participating organizations must agree to provide appropriate security for, and

---

[15] *See* http://www.aboutads.info/.

[16] *See id.*; *see also* http://www.aboutads.info/consumers/.

limit their retention of, data collected and used for behavioral advertising. In our multiple roles as a browser manufacturer, ad network, and website operator, for example, we are coordinating with the Interactive Advertising Bureau and other participants in the Self-Regulatory Program to ensure that this important initiative is effective, enforceable, and broadly accepted. Consistent with our commitment to responsible industry leadership, we also are working at the World Wide Web Consortium, the standards-setting body for the Web, to develop an industry consensus about technical standards that can be implemented across browsers to enable common tools for consumers to control tracking by third parties.[17] As a result of these self-regulatory initiatives, we believe that the online advertising industry is taking important and effective steps toward improving consumer privacy.

While the efforts of individual companies and industry self-regulatory initiatives play key roles in protecting consumer privacy, baseline federal privacy legislation could serve as an effective complement to industry efforts. The current sectoral approach to privacy regulation makes compliance a complex and costly task for many organizations. According to one estimate, by 2009 there were more than 300 federal and state laws relating to privacy.[18] The sector-specific approach also creates confusion among consumers and can result in gaps in the law for emerging sectors or business models. By contrast, baseline privacy protections that apply across sectors could provide more consistent protections for consumers and simplify compliance for businesses that increasingly operate across those sectors. Baseline privacy protections also could promote accountability by ensuring that all businesses use, store, and share commercial data in responsible ways, while still encouraging companies to

[17] *See* http://www.w3.org/2011/tracking-protection/charter-draft.html.

[18] Lee Gomes, The Hidden Cost of Privacy, FORBES, June 8, 2009, available at http://www.forbes.com/forbes/2009/0608/034-privacy-research-hidden-cost-of-privacy.html.

compete on the basis of more robust privacy practices.[19] In addition, baseline federal privacy legislation could foster greater legal certainty by preempting state laws that are inconsistent with federal policy.[20]

If Congress pursues legislation, however, it should be crafted carefully and with two goals in mind. First, it must protect consumers' privacy and data security while enabling innovation and facilitating the productivity and cost-efficiency that new business models and computing paradigms offer. Second, it should create privacy protections that can withstand the rapid pace of technological change so that consumer data is protected not only today, but also in the decades to come. To achieve these two ends, any proposed legislation should be tested against certain fundamental criteria, among them:

- Flexibility. Legislation should permit businesses to adapt their policies and practices to match the contexts in which consumer data is used and shared and be sufficiently flexible to allow technological innovation to flourish. Instead of imposing prescriptive rules, the legislation should establish baseline principles, then permit businesses to adopt methods and practices to achieve those principles in a manner that best serves their business models, technologies, and the demands of their customers.

- Certainty. Legislation should provide businesses with certainty about whether their privacy policies and practices comply with legal requirements. Government-recognized safe harbor programs are one way in which the framework can remain flexible but also provide businesses the certainty necessary to encourage the development of innovative privacy protections and new products and services.

- Simplified Data Flow Standards. Legislation should seek to facilitate the interstate and international data flows that are necessary to enable more efficient, reliable, and secure delivery of services, including through harmonizing international privacy regimes and preempting a patchwork of state privacy laws.

- Technology neutrality. Legislation should avoid preferences for particular services, solutions, or mechanisms to provide notice, obtain choice, or protect consumer data.

---

[19] Even if responsible companies adopt strong practices and participate in self-regulatory initiatives, one bad apple could potentially spoil the whole bunch and undermine trust in online commerce and cloud computing generally. That is where government can play a key role by setting baseline standards and taking enforcement action against bad actors who do not take privacy seriously. Government-recognized safe harbor programs are another way the government can play a critical enforcement role, yet at the same time preserve flexibility and provide businesses with the certainty they need to encourage the development of innovative privacy protections and new products and services.

[20] See., e.g., Remarks of Brad Smith to the Congressional Internet Caucus, November 3, 2005, available at http://www.netcaucus.org/speakers/2005/smith/.

Online advertising is a good example of the need for flexible and technology-neutral baseline principles within a framework that allows for specific self-regulatory initiatives that co-exist with, or build on top of, the baseline obligations of the law. The technologies and business models have been evolving very quickly and will likely continue to change in the coming years. Adopting very specific law based on what online advertising looks like in late 2011 likely would be dated in just a year or two, and could significantly hinder innovation. Instead, a federal privacy law might embody baseline principles of transparency, control and security. But how those are implemented with respect to current technologies and online advertising business models is more appropriately addressed through industry self-regulation and innovative technology tools than prescriptive rules that try to impose a static and one-size-fits-all set of rules on a dynamic and multi-faceted industry.

IV. Microsoft's Support For Consumer Education Efforts

While I have focused my remarks thus far on company best practices, technology tools, and baseline rules of the road established through both self-regulatory efforts and legislation, that focus should not minimize the importance of ensuring that consumers understand data practices and their privacy implications. Indeed, it would be impossible to meet consumer expectations if there were no effort to inform consumers of the protections available, the controls and tools at their disposal, and the practices of the companies with which they are interacting. Informed and educated consumers are much better able to make choices that align to their own privacy needs and sensitivities and to take steps to help protect themselves from harm. That is why we provide consumers with clear information about our own practices and, where appropriate, offer choices about what data will be collected and how it will be used. Additionally, we provide to consumers general educational materials about how to protect their privacy and security and how to stay safe online.[21] We also have partnered with consumer advocates and government agencies to develop educational materials on consumer privacy and data

[21] See, e.g., http://www.microsoft.com/security/default.aspx.

security,[22] and we believe that such initiatives are important for ensuring that consumers understand the importance of protecting their privacy and security online — and that they are equipped with the information and tools with which to do so.

V. Conclusion

Thank you for extending us an invitation to share our experiences and thoughts with you. We commend the Subcommittee for holding this hearing today, and we are committed to continuing to work collaboratively with you, other government stakeholders, members of industry, privacy advocates, and consumers to advance consumer privacy and promote trust in online services. Privacy is a moving target and a complex challenge, but we believe that it is possible to honor individuals' privacy expectations without compromising the nation's strong record of — and ongoing need for — technological innovation.

[22] *See, e.g.,* National Cyber Security Alliance (NCSA), *available at* http://www.staysafeonline.org/; GetNetWise, *available at* www.getnetwise.org; Internet Keep Safe Coalition, *available at* www.ikeepsafe.org; Stop. Think. Connect, *available at* http://safetyandsecuritymessaging.org.

Appendix 1

Microsoft Advertising

AdChoices: Learn about ads

Who delivered this ad to you?

This ad was delivered to you by Microsoft Advertising.

Why are some ads personalized?

To provide you with a more relevant online experience, Microsoft Advertising customizes a portion of the online ads that you see based on your past online activity. Information about your past online activity, or the activity of other people using this computer, might be used to help predict your interests and select the ads that you see.

Where can I learn more about my online information? New

View and manage your online information in the Microsoft Personal Data Dashboard **Beta**.

Where can I learn more about how Microsoft Advertising uses the information that it collects?

For more information about Microsoft Advertising privacy practices and principles, see the Display of Advertising (Opt-out) section of the Microsoft Online Privacy Statement and Microsoft Privacy Principles for Search and Online Behavioral Targeting.

What options do I have about personalized advertising?

You can:

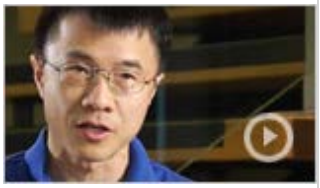
- Opt out of receiving personalized ads on websites that use the Microsoft Advertising Platform and manage your advertising interests with the My Interests tool.
- Opt out of receiving personalized ads from other advertising companies by visiting the Consumer Choice Page.

How can I learn more about online advertising?

For more information about online advertising, see the Understanding Online Advertising page on the Self-Regulatory Program for Online Behavioral Advertising website.

For more information about how online advertising affects your privacy, see

Listen to Microsoft perspectives on online **privacy**, **safety**, and **personalized advertising**.



the Learn More page on the Network Advertising Initiative (NAI) website.

For more information about how Internet Explorer 9 can help maintain your privacy choices, see the Internet Explorer 9 Features page on the Internet Explorer website.

Appendix 2

Microsoft Advertising

Sign in

Personalized Advertising from Microsoft

(Last updated September 2011)

Why are ads personalized?

Personalized ads from Microsoft help provide ads that are more relevant and useful to you. Learn more about personalized ads.

Don't want personalized ads from Microsoft?

If you don't want to see personalized ads from Microsoft, you can choose not to receive these types of ads on websites that use the Microsoft Advertising Platform by selecting the opt-out choice on this page. You can also choose to opt out of receiving personalized ads from advertising companies other than Microsoft, on the Consumer Choice Page.

How can I influence personalized ads?

At Microsoft, we do our best to provide personalized ads that you might find interesting. We don't always get it right, though. With our My Interests tool, you can help us customize your personalized ads by selecting areas that are of interest and not of interest to you.

Note
The ads you see might not always reflect your selected interests. Only a small portion of the ads that we display is personalized, and different factors influence how they're personalized.

If I opt out, what happens?

Opting out does *not* mean you will stop getting ads or see fewer ads; however, if you do opt out, the ads that you receive will no longer be personalized.
In addition, opting out does not stop information from being collected. However, neither this information nor any information collected from you in the past will be used for displaying personalized ads. Microsoft will continue to deliver content that is personalized for you, such as the news articles that are displayed on MSN and the results that appear when you search for software updates.

My Interests

This list is generated based on interests that you have added or removed or that Microsoft has suggested.

Interests are available only after you have signed in with your Windows Live™ ID. Please sign in to manage your interests.

Your opt-out choices

On this computer or device, when you use this web browser: Opt out

You are opted in

On any computer or device, after you've signed in to Windows Live™:

You must sign in before you can update the setting.

On your computer or device, we place the following cookies associated with online advertising:

Cookie for this browser:
Cookie for current user:

Help build the largest human-edited directory on the web.

Submit a Site - **Open Directory Project** - Become an Editor
Directory listings are provided by Open Directory and enhanced by Microsoft.

Give us feedback | Help

Appendix 3

Microsoft Personal Data Dashboard Beta

Sign out

My Profile My Data My Choices More Services

My data

On this page, you can view and manage some of your online personal information.

Interests

Bing searches

More data Coming soon

Your interests

These are topics that you said you like or that we think you might like.

You said you like these topics:

Add more interests

You haven't added any interests yet. To search for topics that might interest you, simply type the keywords in the **Add more interests** box.

You said you dislike these topics:

Add more interests

Do you want to add to your list of dislikes? To search for topics that don't interest you, simply type the keywords in the **Add more interests** box.

We think you might like these topics:

No interests are currently assigned to you.

Data tips

Managing your interests

Interests are topics that you're curious or excited about—like your favorite music, books, and Movies. You can view, confirm, or remove any of the topics in this list.

Interested in other topics?

You can add more topics by using the search box.

 © 2011 Microsoft Corporation

Microsoft Personal Data Dashboard Beta

Sign out

My Profile My Data My Choices More Services

My choices

On this page, you can make choices about how Microsoft uses your data.

Information use is allowed by the following enabled services.

Allowed Microsoft Advertising

More services Coming soon

About Microsoft Advertising

With the Microsoft Personal Data Dashboard, you can choose not to receive personalized ads on websites that use the Microsoft Advertising Platform by not allowing Microsoft Advertising to use your information.

Information used by Microsoft Advertising

The Microsoft Advertising Platform customizes personalized ads based on different types of information, including but not limited to:

Bing searches Interests Profile

What does it mean not to allow Microsoft Advertising to user your information?

Well, first, it doesn't mean you will stop getting ads or see fewer ads; but, it *does* mean that the ads you get won't be personalized anymore. Also, not allowing Microsoft Advertising to use your information doesn't stop information from being collected. This information or any information collected from you in the past is used for displaying personalized ads. Microsoft Advertising does this so it can keep delivering rich content that is personalized for you, for example, the news articles displayed on MSN and the results you get when you search for software updates.

Tips on choices

Personalized advertising from other companies

You can also opt out of getting personalized ads from advertising companies other than Microsoft, on the Consumer Choice page.

AdChoices: Learn about ads

To learn more about personalized advertising and how you can control which ads you see, see the AdChoices: Learn about ads page.

 © 2011 Microsoft Corporation

Microsoft Personal Data Dashboard Beta

Sign out

My Profile My Data My Choices More Services

More services

Here are additional Microsoft services that may store and use your personal user information. Click the link to each service to manage your personal information there.

Windows Live Services

Windows Live provides a suite of services to store and manage your profile information online, including Hotmail, Calendar, Photos, and SkyDrive. For the full list, see the Windows Live directory of services.

MSN Profile

If you created a public profile on MSN, you can edit or delete your profile in the MSN Member Directory.

Microsoft.com Profile

View and manage your microsoft.com profile at the Microsoft.com Profile Center.

Xbox

View and manage your Xbox Live or Xbox.com profile on the page on Xbox.com. My Xbox page on Xbox.com.

Zune

View and manage your Zune or Zune Pass profile by clicking Manage My Account on the profile page of Zune.net.

To learn more about how Microsoft uses your information, please read the Microsoft Online Privacy Statement.

 © 2011 Microsoft Corporation