Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft®

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.	Prospective use: Opt-out choice Retroactive use: 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-out choice
Multi-site Advertising	Online advertising across multiple, unrelated third-party sites.	Pass-through notice: make reasonable efforts to require website operators to link to a privacy notice on their home page
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 privacy notice on home page; follow reasonable security and data retention obligations

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:

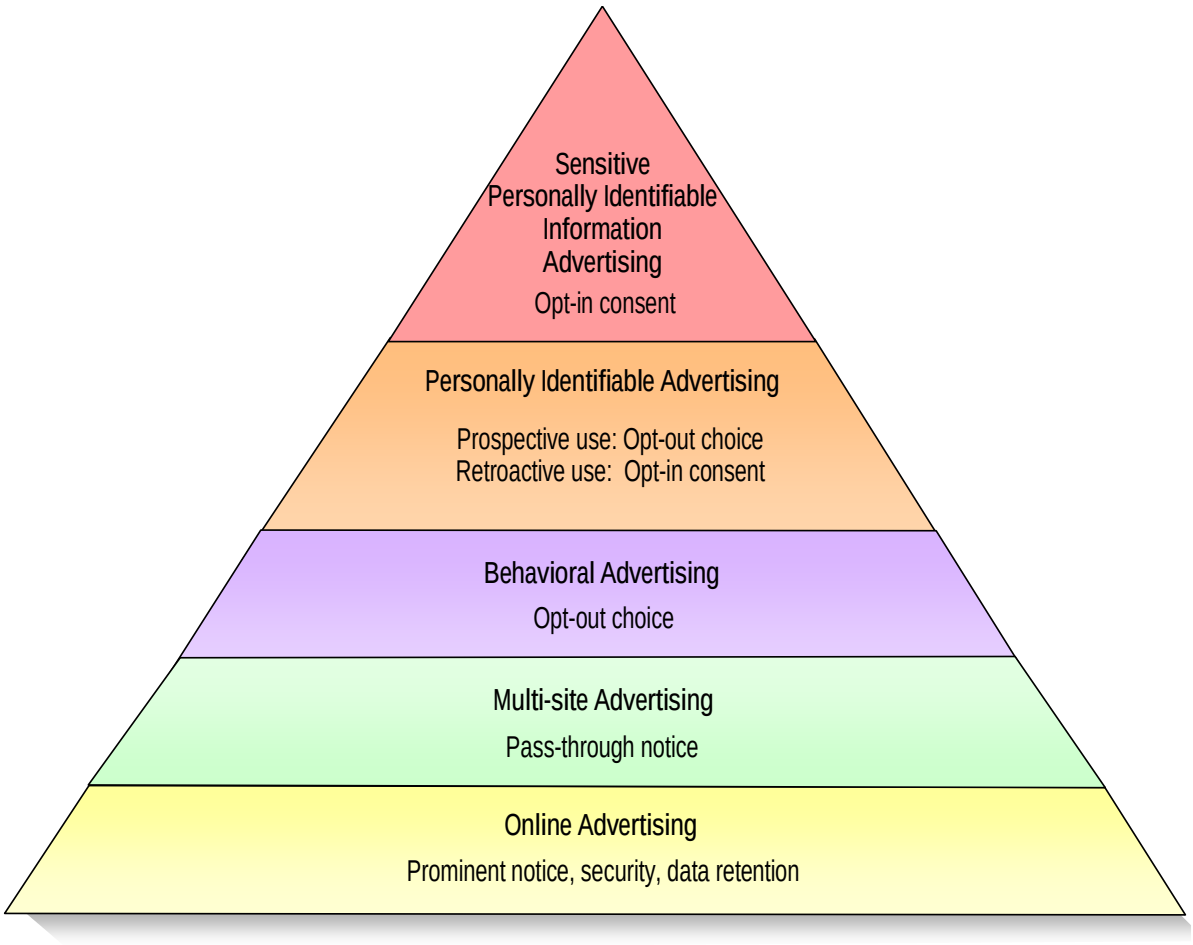
1. Obtain affirmative express consent before using sensitive personally identifiable information for behavioral advertising.

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,

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

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

23 July 2007

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

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

Principle I: User Notice

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

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

Principle II: User Control

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

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

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

Principle III: Search Data Anonymization

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

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

Principle IV: Minimizing Privacy Impact and Protecting Data

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

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

Principle V: Legal Requirements and Industry Best Practices

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

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

Microsoft

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

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 indentifying 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 Live[1]

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.

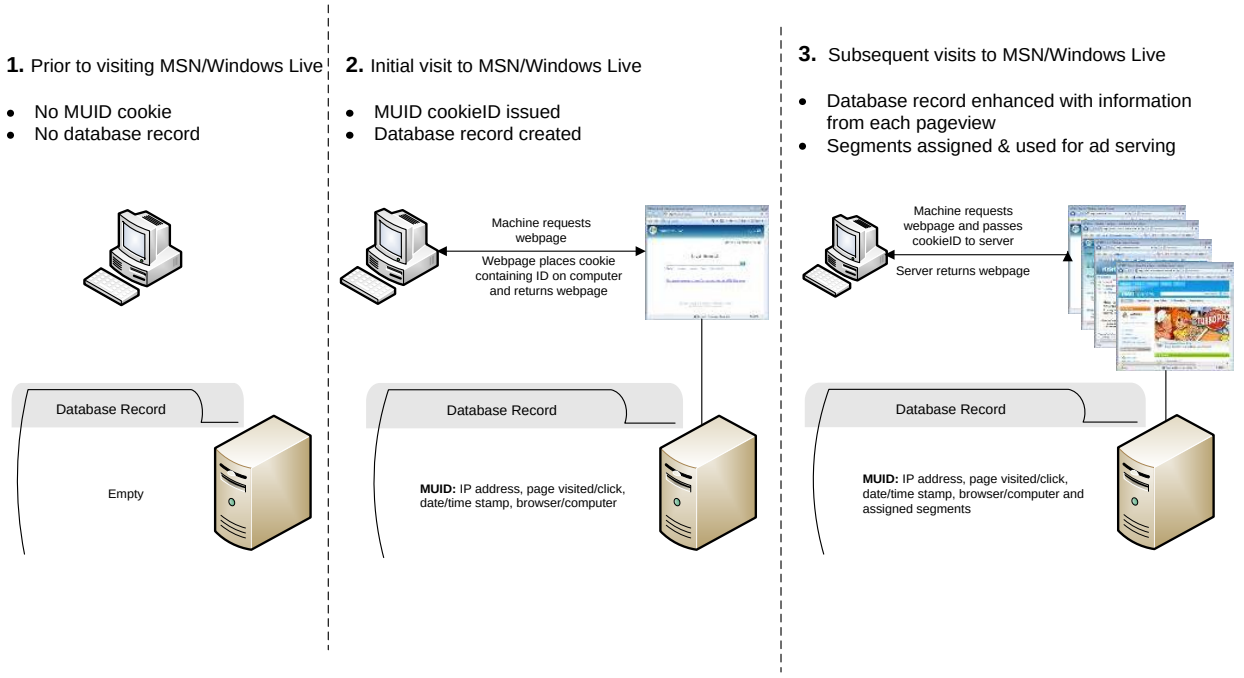


Figure 1. The Machine Unique ID (MUID).

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.

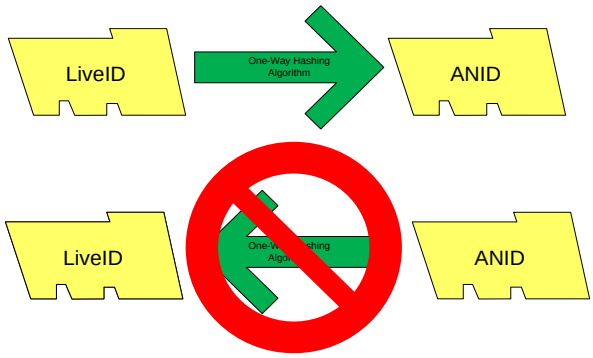


Figure 2. One-way cryptographic hash.

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.

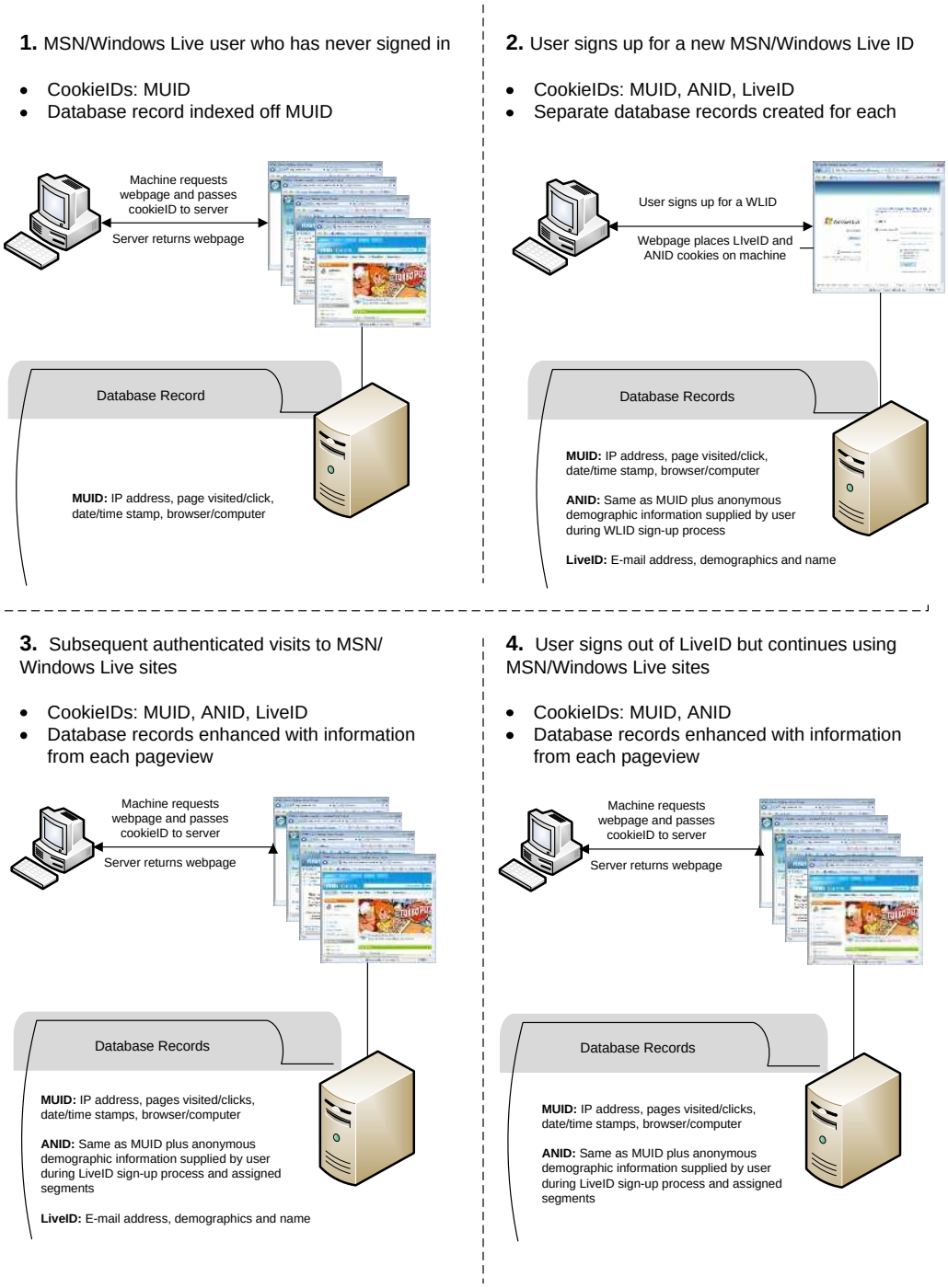


Figure 3. Sample MUID, ANID and LiveID interactions.

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.