Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

February 18, 2011

VIA ELECTRONIC DELIVERY

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-113 (Annex)
600 Pennsylvania Avenue, NW
Washington, DC 20580

*Re: File No. P095416 — Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"*

Dear Secretary Clark:

Microsoft submits these comments in response to staff's request for feedback on its preliminary report on consumer privacy, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" ("Staff Report"). Microsoft commends the Commission for seeking input on this preliminary report and through its successful series of roundtable discussions that explored the privacy challenges posed by new technologies and business practices that collect and use consumer data. Given our long-standing commitment to privacy and data security, Microsoft welcomes the opportunity to participate in this important dialogue and to work with staff, consumer advocates, and others in industry to develop a robust privacy framework that will withstand rapid technological advances while fostering innovation.

## I. INTRODUCTION

For over three decades, the FTC has developed strong privacy and data security protections that have helped build consumer confidence in both offline and online markets. In recent years, however, it has become increasingly evident that dramatic and rapid technological advances are testing how the fundamental principles that underpin consumer privacy and data protection law — such as notice, consent, and reasonable security — should apply.[1]

The explosive growth of the Internet, cloud computing, the proliferation of computers and handheld mobile devices, and the expansion of e-commerce, e-government, e-health and other

[1] *See, e.g.*, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), http://business.ftc.gov/legal-resources/ftc-staff-report-self-regulatory-principles-online-behavioral-advertising.

web-based services have brought tremendous social and economic benefits. And technological advancements and increased computing power have benefited businesses and consumers, both online and offline. At the same time, however, these technologies have fundamentally redefined how, where, and by whom data is collected, used, and shared.

The challenge for industry and governments to address together is how to best protect consumers' privacy and data security while enabling innovation and facilitating the productivity and cost-efficiency offered by new business models and computing paradigms. To help address this challenge, the FTC's privacy framework must achieve two ends. First, it must afford consumers robust privacy protections, while at the same time enabling businesses to develop and offer a wide range of innovative products and services. Second, it must be designed to 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, the proposed framework should be tested against certain fundamental criteria, among them:

- *Flexibility*. The framework must be flexible in order to permit businesses to develop innovative privacy technologies and tools. Flexibility means that businesses can adapt their policies and practices to match the contexts in which consumer data is used and disclosed and the type of relationship that they have with the consumer.

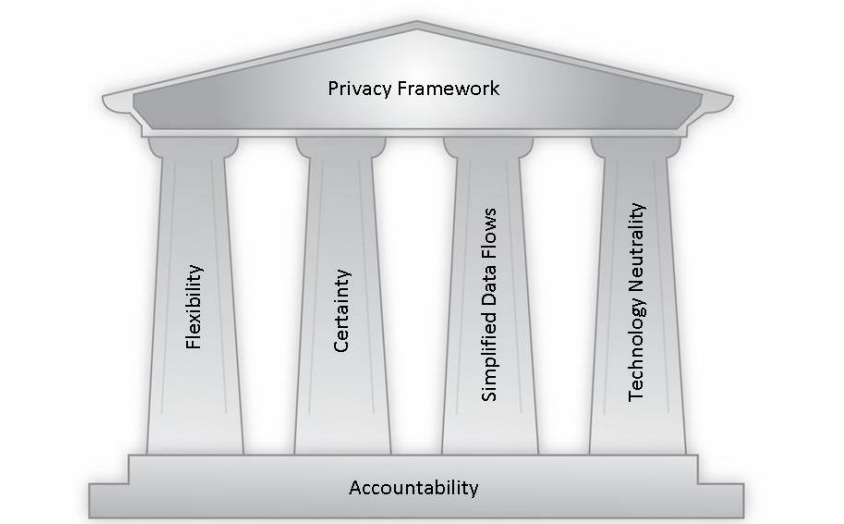
- *Certainty*. The framework must provide businesses with certainty about whether their privacy policies and practices comply with legal requirements. Government-recognized safe harbor programs are one way in which the framework can remain flexible but also provide businesses the certainty necessary to encourage the development of innovative privacy protections and new products and services. The framework also can promote certainty by seeking harmonization with international standards and focusing enforcement efforts on unfair and deceptive practices that result in cognizable consumer harms.

- *Simplified data flows*. The framework must recognize that data is no longer constrained within geographic or business silos to the extent that it was when the FTC first began to focus on privacy issues in the early 1970s. Today, consumer data regularly flows across state and national borders, is shared within company affiliates and with vendors that manage the data on behalf of the company, and may be transferred to third parties that use the data, for example, to provide consumers with information about products and services that may be of interest to them. The framework must facilitate the data flows that are necessary to enable more efficient, more reliable, and more secure delivery of services to consumers at lower prices.

- *Technology neutrality*. The framework must avoid preferences for particular services, solutions, or mechanisms to provide notice, obtain choice, or protect consumer data. There is no question that technology will continue to change — and change rapidly – and the framework must allow companies to adapt to new technologies. Also, preference for one privacy tool over another, for example, could chill innovation by deterring providers from developing alternative or improved approaches to protect consumer data.

In addition, accountability must serve as the foundation for the FTC's privacy framework.[2] Accountability demands that businesses meet privacy goals based on criteria established in current public policy, but permits businesses to adopt methods and practices to reach those goals in a manner that best serves their business models, technologies, and the demands of their customers. By focusing on achieving substantive outcomes, rather than imposing prescriptive rules that may be of limited effect or that may burden businesses without yielding commensurate privacy benefits, the FTC's privacy framework will be more robust and resilient to technological change.

Our overall views and suggestions regarding the FTC's privacy framework are illustrated in the following diagram. The framework should be supported by a foundation grounded in the concept of accountability. Building on this foundation are the four criteria by which the overall privacy framework is measured: (1) flexibility, (2) certainty, (3) simplified data flows, and (4) technology neutrality. These criteria support the framework itself, and, in this manner, industry, the FTC, and other relevant stakeholders can achieve the ends of affording consumers robust privacy protections that can withstand the test of time, but that still enable businesses to offer a wide range of innovative products and services.




Microsoft works hard to ensure that the company's products, services, processes, and systems incorporate measures designed to help protect consumer privacy; that we provide consumers with simple and effective tools to control how their information is accessed, used, and shared; and that our privacy statements are clear and understandable for consumers. As a company that has been focused on consumer privacy for many years, we hope our comments provide the FTC with helpful feedback and useful illustrations that might be more generally considered within the framework. To this end, the next section of these comments responds to the questions raised by staff in Appendix A of the Staff Report, applying the four criteria identified above and the concept of accountability to help develop a dynamic consumer privacy framework.

---

[2] Additional information about the concept of accountability is available at http://www.hunton.com/Resources/Sites/general.aspx?id=330.

## II. COMMENTS ON STAFF'S PROPOSED PRIVACY FRAMEWORK

As an initial matter, the concept of a universal privacy framework is consistent with Microsoft's support for a comprehensive approach to consumer privacy. Beginning in 2005, Microsoft has advocated for comprehensive federal privacy legislation that sets forth baseline privacy protections that are not specific to any one technology, industry, or business model. Like the staff's proposed privacy framework, such legislation would apply both online and offline and would include baseline privacy requirements for transparency, consumer control, and security. Importantly, this legislation also would create legal certainty by preempting state laws that are inconsistent with federal policy.

However, Microsoft does not believe that legislation is a complete solution. Legislation must work in conjunction with industry self-regulation and best practices, technology solutions, and consumer education. While legislation is an appropriate vehicle for setting flexible, baseline standards, it is difficult for legislation to keep pace with evolving technologies and business models. Search and online advertising are examples of such rapidly evolving areas, and we commend the FTC for recognizing the important role that self-regulation plays in the context of online behavioral advertising.[3]

With this background in mind, provided below are Microsoft's comments on the various elements of the proposed privacy framework, grouped by the headings that staff use in Appendix A of the Staff Report.

### A. Scope

The Staff Report first asks whether there are any practical considerations that support excluding certain types of companies or businesses from the scope of the privacy framework. In connection with our calls for comprehensive federal privacy legislation, Microsoft has recognized that an exception for certain businesses may be warranted where the amount and intended use of the consumer information presents an especially low risk. Specifically, we have supported a limited exception for companies that collect, use, store, or disclose personal information from fewer than 5,000 individuals in any twelve-month period and use such information only for purposes that are reasonably necessary for the operation of the company, such as product fulfillment, protecting the rights of the company and third parties, and first-party marketing. Such an exception should be based on the nature and amount of the data, rather than the size of the business, since even very small businesses can handle enormous amounts of data or highly sensitive data, and the same privacy protections should apply to such activities. Staff's suggestion that any such exception should be limited to non-sensitive data is consistent with this risk-based approach.

The remainder of staff's questions in this section touch on the challenges of data anonymization and the fact that many anonymization methods have been called into question in recent years.[4] Anonymization, pseudonymization and de-identification methods come in various strengths and

---

[3] *See, e.g.*, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), http://business.ftc.gov/legal-resources/ftc-staff-report-self-regulatory-principles-online-behavioral-advertising.

[4] *See, e.g.*, Paul Ohm, "Broken Promises of Privacy: Responding To the Surprising Failure of Anonymization," 57 UCLA L. REV. 1701 (2009-2010).

have a spectrum of uses ranging from general risk mitigation to securing highly sensitive information. While technologies that focus on risk mitigation ultimately may be overcome by a determined and highly skilled adversary, they still can provide a meaningful tool in many circumstances to help manage risk – particularly if combined with other risk-mitigation steps and used as part of an overall privacy program that includes, for example, access controls and reasonable limitations on data retention. Businesses should have the flexibility to select appropriate anonymization or de-identification methods based on the context, including the type of information that is being collected, how this information will be used, and the relationship that the business has with the consumer.

In the online advertising context, for example, Microsoft uses a de-identification technique to separate the data used for ad targeting from any information that personally and directly identifies individual consumers.[5] Specifically, for consumers 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 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 identifier, rather than an account identifier that could be used to personally and directly identify a consumer. In addition, we have implemented policies and technical measures designed to prevent the unauthorized correlation of this information and to protect the information we collect and maintain.

In the search context, in addition to using this de-identification technique to keep search query data separate from any identifiable account information,[6] Microsoft applies additional levels of pseudonymization and anonymization at different points in the data lifecycle. In particular, we will permanently remove the entirety of the IP address from all Bing search query data after 6 months. Then, at 18 months, we take the additional step of deleting all other cross-session identifiers, such as cookie IDs and other machine identifiers, associated with the search query.[7] We believe that this approach strikes an appropriate balance based on the need to store data about search queries in order to protect against security threats and improve our services and, in light of our robust de-identification and anonymization efforts, to provide a strong approach to protecting consumer privacy.

In other contexts, however, different anonymization processes may be more appropriate. As noted above, a number of factors should be considered in determining what strength of

---

[5] A white paper describing Microsoft's "de-identification" process is available at http://www.microsoft.com/privacy/policymakers.aspx.

[6] This separation does not apply when users opt to sign-in to the Bing search service and save their search history in association with their Windows Live ID.

[7] The presence of cross-session identifiers could permit the correlation of sufficient search data related to an individual consumer to make it possible to identify such an individual even without an IP address or without what would traditionally be considered personally identifiable information. Further, partial approaches — such as removing only portions of an IP address — are inadequate in the search context because a partially redacted IP address can still narrow the field of computers from which an associated search could have originated, and this information, combined with other data, could be used to re-identify a search query. Thus, we believe that, in order to provide the strongest privacy protections and make search query data truly anonymous, all cross-session identifiers must be removed in their entirety from the data.

anonymization is needed, including the privacy risk that is being mitigated, the type of information that is being secured and the other privacy protections that may be in place.

Finally, it is worth noting that concepts emerging from the research community may be useful in the future to support a number of scenarios related to anonymization or de-identification. For instance, one area of research yields the possibility of querying some types of databases that may contain information that could identify an individual in such a way that the values computed and released via the query would reveal essentially no information about whether the computation used the data of any given individual, no matter what external information is available or becomes available in the future. Researchers at Microsoft Research are recognized leaders in one mathematically rigorous formulation of this approach known as differential privacy. There are limitations to the existing mathematical techniques for achieving differential privacy, and the research is ongoing. However, differential privacy virtually eliminates the risk that the results from a query to a database can be cross-correlated with other databases to reveal the identity of an individual.[8]

### B. Promoting Consumer Privacy Throughout Organizations and at Every Stage of the Development of Products and Services

The Staff Report encourages businesses to adopt a "privacy by design" approach that would require businesses to provide consumers substantive privacy protections and to maintain comprehensive data management procedures. Microsoft's commitment to privacy by design is deep and long-standing. Privacy by design is an integral part of how we demonstrate our accountability, and describes not only how we build products, but also more broadly how we operate our services and conduct our business.

For instance, Microsoft was one of the first companies to appoint a chief privacy officer, an action we took nearly a decade ago, and we currently employ over 40 employees who focus on privacy full-time, and another 400 who focus on it as part of their jobs. In addition, we have a robust set of internal policies and standards that guide how we do business and how we design our products and services in a way that respects and protects consumer privacy.[9] We use these standards and our privacy infrastructure as part of our Trustworthy Computing initiative to engineer privacy into our products and online services from the outset, review all products and services to identify privacy issues at an early stage, and encourage the continued consideration of privacy and data security throughout the project lifecycle – including after the release of the product or service into the market.

---

[8] *See* http://research.microsoft.com/en-us/projects/DatabasePrivacy/ for more information on differential privacy.

[9] For example, Microsoft's Privacy Guidelines for Developing Software Products and Services, which are based on our internal privacy standards, are available at http://www.microsoft.com/privacy. We make these standards publicly available for other organizations to use to develop and guide their own product development processes. To encourage industry to adopt these guidelines, we have taught courses for others in industry to educate them on the standards. And our privacy guidelines are part of the foundation for one of the International Association of Privacy Professional's privacy certifications – the Certified Information Privacy Professional for IT (CIPP/IT). *See* https://www.privacyassociation.org/images/uploads/CIPP_IT_Reading_List_0909.pdf.

Accordingly, Microsoft supports an industry-wide privacy-by-design principle that encourages businesses to incorporate privacy protections into their data practices and to develop comprehensive privacy programs. The Staff Report appropriately recognizes that "[t]he size and scope of [privacy] programs should be appropriate to the risks presented to the data," so that "companies that collect and use small amounts of non-sensitive consumer data should not have to devote the same level of resources to implementing privacy programs as companies that collect vast amounts of consumer data or data of a sensitive nature."[10]

However, businesses need flexibility not only for developing privacy programs, but also in implementing privacy-by-design principles more broadly. Specifically, Microsoft urges the Commission to avoid imposing prescriptive requirements with respect to data retention periods or in further defining "specific business purpose" or "need."[11] Rather, any limitations on data retention and use must focus on accountability and on accommodating and encouraging evolving or innovative technologies and business models over time. This is because there are a number of legitimate business reasons for retaining and using consumer data. 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. Accordingly, what is a "reasonable" data retention period or "business purpose" will vary widely and will depend, for example, on each business's unique data needs, the types of information involved, the nature of the consumer relationship, and whether the business has implemented other privacy and security protections.

### C. Commonly Accepted Practices

The Staff Report raises a number of questions regarding its proposal to identify a limited set of "commonly accepted practices" for which companies would not be required to obtain consent. An illustrative list of commonly accepted practices may provide industry with some certainty about when choice is unnecessary and may help guide industry in developing useful and appropriate mechanisms for consumer control. In this regard, we commend staff for moving towards a "use and obligations" model with respect to the framework's consumer choice requirements. Under this model, the decision to use information creates legal obligations on the business that uses the information. This model is appropriately flexible because legal obligations will vary depending on context and the level of risk associated with the use.

Any attempt to create a list of "commonly accepted practices" should take into account that what is "commonly accepted" changes over time, sometimes fairly rapidly, as technology, business models, and consumer adoption and usage of services evolves. For example, a decade ago few consumers were publicly sharing their personal photographs and home videos, but today consumers regularly post these materials on social networking and online video websites without hesitation because they believe such services are valuable. In addition, what consumers accept as a common practice greatly depends on many different factors such as the industry sector involved (e.g., automotive, health) or on whether the consumer has an established relationship with the business.

---

[10] Staff Report, at 49.

[11] Staff Report, at A-1 (asking whether there is "a way to prescribe a reasonable retention period" and whether "specific business purpose" or "need" should be further defined).

To the extent the FTC decides to create and maintain an illustrative list of commonly accepted practices, we suggest that the following practices be added to the FTC's list:

- Detecting, preventing, or acting against actual or suspected threats to the business, third parties, or the product or service. Microsoft supports staff's inclusion of fraud prevention in the proposed list, but believes the list should go further to include all threats. This includes, for example, security attacks, phishing schemes, and spamming.

- Carrying out an employment relationship with the individual.

- Using the name, title, or business contact information for an employee of any public or private entity to contact that individual for any purpose within the scope of the individual's professional activities.

- In connection with a corporate merger, or a stock or asset acquisition, where the successor company will be engaged in a similar line of business and the consumer's information will continue to be used and disclosed only for purposes consistent with those for which it was originally collected or subsequently authorized.

- Other uses that the individual reasonably would expect under the circumstances.

In addition, Microsoft agrees with staff's proposal that sharing data with commonly branded affiliates should be considered first-party marketing.[12] Specifically, a corporate entity should be allowed to disclose consumer data to its parent company, a controlled subsidiary, or an affiliate or other organization under common control, as long as the organization operates under common or substantially similar internal policies and procedures (which includes compliance with the privacy notice(s) presented to the consumer). This approach promotes simplified data flows because corporate affiliates often need access to the data to complete a requested transaction or to provide consumers related products and services that may be of interest to them. In addition, such entities often share back-end database systems, and consumers reasonably would expect that these entities are the same or closely related.

The Staff Report also asks how the proposed framework should apply to data "enhancement," whereby a business combines data obtained from other sources with its own consumer data. In these circumstances, Microsoft believes responsibility should be shared so that the data provider remains responsible for complying with the framework's requirements with respect to the sharing of the data, whereas the entity that receives the data for enhancement purposes is responsible for complying with the framework's requirements with respect to any subsequent use of the data.

### D. Practices That Require Meaningful Choice

For any practice that is not "commonly accepted," the Staff Report states that businesses should offer consumers choice at the time and in a context in which the consumer is making

[12] Staff Report, at 55.

a decision about his or her data. Microsoft strongly supports the notion that the most appropriate and effective method for offering consumers choice will depend on context. Microsoft disagrees, however, that to be most effective, choice must always be offered "just-in-time."

In our products and services, we currently provide prominent notice and opportunities to exercise choice before data is collected. Sometimes this choice is provided "just in time," such as when we ask a consumer whether he or she would like to turn on the Suggested Sites feature in Internet Explorer 8. In the online advertising context, we have been supportive of a uniform icon or graphic that provides close-in-time choice for behaviorally targeted ads, and we have started implementing the "ad choices" icon developed by the Interactive Advertising Bureau and the Network Advertising Initiative.[13]

In other contexts, however, we believe it is more appropriate to offer a set of privacy choices before the consumer actually encounters the relevant feature. For example, we obtain consent to turn on a number of features during the initial launch of Windows 7 on a new or updated personal computer, including certain privacy features in Internet Explorer, the Windows Update functionality, online help, and several others. Consumers are likely to be most focused during installation on the features of their new operating system, and our experience shows that this is the best time to ask consumers to consider a range of features that they might want to enable. By considering these features together, they may be more likely to reflect on all of the possible configurations and be able to more easily compare alternatives.

Further, requiring "just in time" choice in many contexts would create a disruption at a time when the user is focused on completing a particular task and is therefore less likely to focus on a privacy choice. In the web context, for example, a consumer may visit a dozen websites or more in a single browsing session; obtaining "just in time" choice every time a new website or page is visited (as opposed to persistent choices through browser controls or an industry opt-out page) likely would only frustrate the consumer, who might begin to click "accept" out of habit in order to quickly get to his or her desired destination. Based on our experience and consumer feedback, we have made a concerted effort over the years to simplify choices for consumers and to interrupt their experience with pop-up notices as infrequently as possible.

Accordingly, Microsoft urges staff to avoid an over-emphasis on "just in time" choice. The framework's clear preference for "just in time" options over other choice mechanisms is inconsistent with the criteria of technology neutrality and flexibility – especially in the context of a rapidly evolving technology environment. Depending on the context, other mechanisms may provide more meaningful or useful opportunities for exercising choice. In addition to the upfront choice example provided above, privacy controls or settings that the consumer can access at any time (such as the Windows Live privacy controls that allow consumers to choose exactly what information they want to share and with whom) can be quite effective and simple to use.[14]

---

[13] *See* http://www.iab.net/media/file/CLEAR_Ad_Notice_Final_20100408.pdf. By clicking the "ad choices" link, consumers are given information about the entities that are responsible for the ad and are provided an opportunity to opt out of behavioral advertising. *See also* http://www.aboutads.info/choices/.

[14] *See* http://windowsteamblog.com/windows_live/b/windowslive/archive/2010/06/17/giving-you-more-meaningful-choices-to-control-your-privacy.aspx.

Further on the topic of consent, the Staff Report also asks (1) whether "take it or leave it" choice is ever appropriate, (2) how choice should be offered with respect to sensitive data and sensitive consumers, and (3) whether enhanced consent should be required for the collection and use of information about teens.

1. "Take It or Leave It" Choice

"Take it or leave it" choice can be appropriate where the use of the information is made clear to the consumer through robust notice. As long as the "deal" is clearly stated (e.g., "This service is available at no charge to you as long as you agree to receive a monthly member letter or to have your registration information used to customize advertising"), and the deal is acknowledged by the consumer through some means appropriate for the context, there is no clear policy reason for prohibiting such a practice. Indeed, permitting "take it or leave it" choice is a technology-neutral and business-model-neutral approach because it avoids preferring subscription or pay services over those that are supported by advertising.

2. Choice Involving Sensitive Data and Sensitive Consumers

The Staff Report asks how "the scope of sensitive information and sensitive consumers [should] be defined and what is the most effective means of achieving affirmative consent in these contexts." This question has no simple answer because what is sensitive for one consumer may not be sensitive for another, and because the ability for sensitive consumers to provide effective choice may vary based on the circumstances. Because of these difficulties, Microsoft encourages staff to avoid adopting rigid definitions or approaches, which are likely to be viewed as both under- and over-inclusive, and instead to provide guidance that recognizes that any obligations will depend on context.

3. Choice Involving Teens

Congress explicitly addressed the issue of children's privacy when it enacted the Children's Online Privacy Protection Act in 1998.[15] At that time, Congress made the determination that special consent requirements should apply only to children under the age of 13. This determination is just as valid today, in part because enhanced consent requirements for teens would create a number of practical challenges. For example, there are no effective mechanisms today for reliably determining an online consumer's age. Rather, website operators rely on self-reporting, which, as COPPA has taught us, is not always reliable. Even more so than young children, teens are likely to falsify their age information in order to avoid barriers to using the service. Consequently, Microsoft urges the Commission to explore alternate means of addressing issues unique to teens, such as targeted educational efforts, rather than imposing enhanced consent requirements for teens.

**E. Special Choice for Online Behavioral Advertising: Do Not Track**

The Staff Report advocates adoption of a "do not track" mechanism and clearly expresses a preference for a method that would "involve placing a setting similar to a persistent cookie

[15] 15 U.S.C. §§ 6501–6508.

on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements."[16]

Microsoft believes that consumer choice is best promoted when there is a wide range of universal choice mechanisms available on the market and businesses have room to innovate in this area. Every actor in the online advertising ecosystem has a role to play in providing consumers greater control over their personal information. In our capacity as both a browser vendor and as an ad network, for example, Microsoft is committed to developing and supporting a number of innovative tools, discussed in greater detail below, that give consumers greater control over the collection and/or use of information about their online actions.

Accordingly, we urge staff to remain technology neutral and to avoid preferring any particular "do not track" mechanism over others. Given how rapidly behavioral advertising evolves — both with respect to the business models and the underlying technologies — there can be no silver-bullet solution. Attempts to require the use of a particular "do not track" technology may quickly become obsolete and could chill innovation in the development of new technologies and mechanisms for providing consumer choice.

In lieu of "do not track" mandates that require the use of a particular mechanism or technology, Microsoft urges the Commission to continue to support industry and self-regulatory efforts at developing universal choice mechanisms.

- Browser-Based Tools

As noted above, the Staff Report shows a clear preference for a browser based do-not-track solution that involves a setting akin to a persistent cookie that every website, ad network, and other third parties would have to read, interpret and respect. As a web browser vendor, Microsoft certainly agrees that browser-based tools can provide consumers with powerful privacy controls, and we believe that ongoing innovation in browser tools should be encouraged. Accordingly, we urge the Commission to avoid endorsing one type of browser-based tool over other tools.

Microsoft has designed Internet Explorer to enable consumers to manage what details of their online activities are maintained, block unwanted communications, and protect themselves against potentially dangerous online content. For example, we have long provided tools that allow users to block cookies or clear their locally stored browser history. In Internet Explorer 8, we introduced the InPrivate Browsing and InPrivate Filtering options to provide consumers even more powerful control over what details are maintained about their online activities. InPrivate Browsing helps prevent a consumer's browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser, thereby leaving virtually no evidence of the consumer's browsing or search history. And InPrivate Filtering provides an additional level of control by allowing consumers to prevent a site from sending details about their visit to third parties that might then use this data to track their browsing activity across the Internet.

[16] Staff Report, at 66.

While the privacy features in Internet Explorer 8 represented significant advancements in the design of browser privacy controls, we continued to look for innovative ways of enabling consumers to exercise more control over their online privacy. The results of these efforts are showcased in the next generation of our web browser, Internet Explorer 9, which will offer a ground-breaking privacy feature, "Tracking Protection." Tracking Protection gives consumers unprecedented control over the collection and use of their data online by allowing consumers to decide which sites can receive their data and by filtering content from sites identified as privacy threats. It does so on the basis of Tracking Protection Lists that identify websites which are, in the view of the list creator, trustworthy and untrustworthy. A Tracking Protection List may include "do not call (or visit)" lists that will block third-party content, including cookies and similar files, from any site that is on the list, unless a consumer visits the site directly by clicking on a link or typing its web address. By limiting calls to these websites, Internet Explorer 9 will limit the information these third-party sites can collect about web users. At the same time, Tracking Protection Lists can include "OK to call" entries that permit calls to specific sites, which allows consumers to create exceptions in a given list.

Anyone on the web (including consumer groups and privacy advocates, enterprises, security firms, and consumers) will be able to create and publish Tracking Protection Lists – which are simply files that can be uploaded to a website and made available to others via a link. Consumers can create or subscribe to more than one list if they wish, and can subscribe and unsubscribe to lists as they see fit. Internet Explorer 9 will automatically check for updates to a consumer's lists on a regular basis. And once a consumer has subscribed to a list or lists, Tracking Protection will remain enabled across all browsing sessions; it will only be disabled when the consumer chooses to turn it off.

More recently, other browser manufacturers – Google[17] and Mozilla[18] – also have announced new do-not-track initiatives. While all three solutions represent progress toward providing consumers with clearer, more understandable and usable tools to help protect their privacy on the web, Internet Explorer's Tracking Protection is a more effective solution because it blocks connections with the third-party sites. It therefore prevents the data collection, as opposed to signaling that there should be limits on the data use. Similarly, Tracking Protection does not depend on websites and ad networks reading, interpreting and respecting a do-not-track header or an opt-out cookie and does not require government enforcement mechanisms. In addition, it provides more comprehensive protection against all types of tracking on the Internet – not just tracking based on cookies or tracking only for online behavioral advertising purposes, and its reach is not limited to participants in a particular self-regulatory program.

---

[17] Google's Chrome extension – "Keep My Opt-Outs" – protects the opt-out cookies based on the Self-Regulatory Program for Online Behavioral Advertising. However, this approach is limited to those companies that participate in the self-regulatory program and requires each of those participants to read and respect the opt-out cookie. Additionally, the extension does not directly address tracking by technologies other than cookies.

[18] Mozilla has proposed adding a "Do Not Track" HTTP header to Firefox that, when enabled, will provide a signal to websites and advertisers that the consumer does not want to be tracked for online behavioral advertising purposes. However, web servers are currently not designed to read the header, so website developers and ad networks would need to enable changes to their servers to look for the header. Additionally, even if advertisers and websites can read the header, it is not yet clear what types of actions websites should take or refrain from taking when the header is enabled.

- Ad Network-Based Tools

In its capacity as an ad network, Microsoft has sought to promote consumer control through a number of industry self-regulatory initiatives that provide meaningful privacy choices for consumers. For example:

  - Microsoft has long been a member of the Network Advertising Initiative, an association of ad networks that maintains an industry opt-out mechanism for behavioral advertising.[19]

  - More recently, Microsoft has been a strong supporter of the Self-Regulatory Program for Online Behavioral Advertising, which includes a set of principles and an educational website where consumers can learn about online advertising and can opt out of having their information used for behavioral advertising.[20] This initiative is intended to provide consumers a "one-stop-shop" where they can opt out of online behavioral advertising from participating networks or take advantage of more granular choices on a per-network basis.

These initiatives are positive steps toward providing consumers simple and efficient opportunities to exercise choice. These industry initiatives could be considered universal choice mechanisms, as they give consumers a single place where they can opt-out of targeted advertising by the key players in the online advertising industry.[21] To the extent there are outliers who refuse to participate in broadly adopted industry self-regulatory programs (*i.e.* a handful of companies collecting or using data in ways that participating companies cannot), it is worth considering whether such refusal could be considered an unfair trade practice, actionable by the FTC under existing law.

Staff also ask whether universal choice mechanisms should "be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications." To the extent technically feasible, Microsoft believes that universal choice mechanisms for behavioral advertising should be technology neutral. However, to the extent there are significant differences in how the technology functions, implementation of these methods may need to vary from one context (e.g., browser-based environments) to the next (e.g., mobile application environments).

---

[19] *See* http://www.networkadvertising.org/index.asp.

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

[21] In addition to these industry initiatives aimed at creating simple, universal choice mechanisms, Microsoft has also developed and provided even more robust choice mechanisms specific to our own ad network. For example, we give consumers the option of tying their opt-out choice to their Windows Live ID, such that it is tied to a person rather than just to a cookie on a particular computer, and thereby making the choice more persistent and allowing it to roam across devices. Microsoft also offers controls that allow consumers to make more granular choices by selecting and de-selecting interest categories as an alternative to entirely opting out of behaviorally targeted ads.

### F. Improved Privacy Notices

The Staff Report asks a number of questions to identify how privacy notices can be made to be clearer, shorter, and more standardized. Microsoft has been at the forefront of industry efforts to promote transparency in the online space.

We have found that transparency requires a careful balance between providing specific, accurate and complete information, drafting disclosures to be easily consumable and understandable, and providing them at a time and in a manner where they are most likely to be noticed and understood. Thus, Microsoft has sought to provide privacy information through a variety of methods. For example:

- Microsoft was 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, which includes the concepts of purpose specification and use limitation.[22]

- In the context of online behavioral advertising, Microsoft has supported, and has started implementing, the recently launched Self-Regulatory Program for Online Behavioral Advertising, which includes placing an "About our ads" link on the bottom of pages that serve ads or collect data used for behavioral advertising and displaying a standardized text link or icon prominently in or next to ads. By clicking on the text link or icon, consumers can easily learn about online behavioral advertising and the privacy practices associated with the particular advertisements they receive, and they can opt out of behavioral advertising if they choose.

- Microsoft has successfully employed in-context, or just-in-time, notice in many of our products and services. For example, Windows Phone 7 includes a geo-location feature that enables consumers to take advantage of the increasing array of location-based applications and services on the market. However, before an application may gain access to a consumer's location information, the consumer is provided clear notice and is asked to provide affirmative consent.

- In an effort to further increase transparency, Microsoft has also published detailed information about privacy practices in white papers,[23] audit reports,[24] and various other forms.

There is no one-size-fits-all approach to effectively providing notice and increasing transparency. Privacy statements are not always the only, or the best, way to convey important

---

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

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

[24] *See, e.g.*, http://www.jeffersonwells.com/DefaultFilePile/ClientAuditReports/Microsoft_PF_IE7_IEToolbarFeature_Privacy_Audit_20060728.pdf.

information about privacy practices to consumers.[25] As we explained above, while "just-in-time" notices provide an effective way to provide notice in many contexts, in other contexts this approach can prove to be too disruptive to the consumer's experience, and other methods may be more effective.

Business models and technologies may be complex, evolve quickly, and involve multiple entities that collect and handle data. Further, there is a wide variety of user interfaces and device functionality in, for example, personal computers, televisions, and mobile devices. As a result, any transparency requirements should be flexible and leave room for innovation. Standardization may only stifle attempts to innovate in ways that foster transparency. For these reasons, standardized or machine-readable approaches for privacy notices have not proven to be widely useful or successful. Overly prescriptive rules requiring standardization of privacy notices may lack the flexibility needed for diverse and rapidly evolving technologies and business models.

While we support an obligation for businesses to provide clear and thorough notices, creating prescriptive and inflexible rules in this area is unnecessary, since the FTC can and does address material failures by companies to provide accurate information about the purposes and uses of the commercial data they collect under Section 5 of the FTC Act. Microsoft urges the FTC to focus its efforts on defining outcomes that promote accountability, rather than on prescriptive requirements that can hamper innovation.

### G. Reasonable Access To Consumer Data

The Staff Report asks a number of questions to help identify what the appropriate scope of a reasonable access requirement might be. Microsoft generally supports giving consumers the ability to access data about themselves; however, any obligation to provide access must be flexible, be reasonable in scope, and reflect technical realities.

Specifically, a reasonable access requirement should apply only to information that is reasonably accessible in the ordinary course of business (as opposed to data that may be located on a backup tape; in an aggregate, pseudonymous or de-identified form; or in a format that makes it infeasible or unduly burdensome to locate or retrieve the data). In addition, while companies can and often do choose to provide broader access to data, reasonable access should be *mandated* only in those instances where the information may be used for purposes that could materially harm or deny a benefit

[25] It is widely noted that full privacy statements are not frequently read by consumers. This realization often leads to calls for privacy statements to be shorter in an effort to make it more likely consumers will read them. But consumers are not the only audience for a privacy statement, and providing notice to consumers is not the only purpose they serve. They also create greater accountability. Regulators can read them and hold companies accountable under existing laws governing unfair and deceptive trade practices. Privacy advocates and journalists can use them to compare practices among different companies. But these accountability objectives can be achieved only if the privacy notices are complete and sufficiently detailed – and that sometimes means they can be quite long. So shortening privacy statements in an attempt to achieve one objective may come at the expense of another. But both these objectives (effective consumer notice and accountability) can be achieved by adopting multifaceted approaches to notice and transparency.

to the consumer. Otherwise, a business should be permitted to provide, upon request, a general notice or a representative sample of the types of information that the business typically collects.

Further, any reasonable access requirement also should be subject to reasonable exceptions. At minimum, a business should be permitted to decline a consumer's request for access if:

- The consumer requesting access cannot reasonably verify his or her identity as the person to which the information relates;
- The privacy or other rights of persons other than the consumer would be violated;
- The burden or expense of providing access would be disproportionate to the risks of harm to the consumer in the case in question;
- Proprietary or confidential information, technology, or business processes would be revealed as a result;
- Revealing the information would likely affect litigation or a judicial proceeding in which the business or the consumer has an interest; or
- Revealing the information would be unlawful, or would likely interfere with the detection or prevention of unlawful activity.

Microsoft does not object to allowing businesses to charge consumers a reasonable fee for accessing the collected information. A fee should be considered "reasonable" if it does not exceed the greater of (1) the actual cost to the business of responding to the consumer's access request or (2) the average cost to the business of responding to similar access requests. Allowing businesses to charge such a fee provides them with some certainty that the access requirement will not become unduly burdensome, and it could help thwart access requests that are unauthorized or that are intended to harass the business recipient (e.g., a campaign to flood a particular business with thousands of detailed access requests).

However, we believe a requirement that companies inform individual consumers of the specific identity of others with whom the company has shared data about that consumer, as well as the specific source of each piece of data goes too far and could be unduly burdensome for companies to implement. Privacy notices certainly should inform consumers in general about the types of entities with whom the company shares data, as well as the types of sources of data the company uses. But requiring the company to identify specific companies and sources with respect to a specific consumer would require businesses to perform a much more detailed level of data tagging and tracking of every piece of data than may be feasible in today's complex ecosystems, and ironically could require the collection and retention of more information about the consumer than is necessary today.

In addition, while businesses should be encouraged to provide access to the data in a format that is usable to the consumer, businesses ultimately should be afforded the flexibility to choose in which format the data will be provided. In general, the richer the data format, the more likely it is to be associated with the specific functions of a service or application (such as a documented email storage format like PST), which may mean that it is directly accessible by a smaller number of services or applications. In contrast, the more widely a format can be used (such as the MIME email storage format), the less likely it is to be able to fully reproduce features such as layout, format, and images in

the way the consumer originally provided them. The choice of which format should be used involves technical and commercial trade-offs that the business is best situated to assess.

### H. Material Changes

Staff request information about the types of changes businesses make to their policies and practices and the types of changes they regard as material. The types of changes companies make range from minor stylistic changes, to changes that address only new services or features, to changes that represent major substantive changes to previous representations about information usage and sharing. We believe that companies could benefit from greater clarity about what types of changes should be considered material, and what obligations should apply in such cases.

In general, we believe that whether a change is material should be based on the reasonable expectations of the consumer. More specifically, a change should be considered material if, after having collected data from a consumer pursuant to a privacy notice, the business seeks to use or disclose such information for a new or expanded purpose, other than a purpose that is reasonably necessary for the operation of the business (such as the commonly-accepted practices discussed in the Staff Report and those we propose above), that the consumer, acting reasonably under the circumstances, would not expect based on the business's prior privacy notice or any consumer consent previously provided.

Further, we believe whenever a business subjects previously collected data to a new or expanded practice that is materially different from a statement made in the previous privacy notice, the business should not only update its privacy notice, but also should provide a clear and prominent statement indicating that the business's privacy notice has been updated and describing the specific purposes for which the information may be used and the manner in which the individual may access the updated privacy notice. In addition, where appropriate, the business should obtain some manner of consent from the consumer to use the information for the materially different practice.

However, while we believe greater guidance and certainty would be beneficial in this area, we encourage the Commission to retain flexibility and allow businesses to determine how best to provide greater transparency and seek consumer consent in cases where a material change warrants doing so. Even within the scope of changes that could be deemed material, there is a range of different contexts and levels of sensitivity, including (1) whether the change benefits consumers by, for example, enabling new functionality in a service; (2) whether the change involves an internal use of the information or a disclosure to a third party; (3) whether the change fosters competition in the marketplace; or (4) whether the affected data is particularly sensitive in nature. These factors and others may justify differing approaches to notice and consent, even where the change is deemed material; and we believe that technical neutrality and reasonable flexibility are essential.

### I. Consumer Education

Microsoft agrees with staff that consumer education is a critical piece of any comprehensive privacy framework, and we will continue to support consumer education efforts to inform consumers of how to best protect themselves and their information online. As an example of our commitment to consumer education, we have developed our own privacy website at www.microsoft.com/privacy which is full of information about our privacy principles, how we approach

privacy by design and other privacy topics, and it is constantly updated with new research findings, white papers and other consumer and policymaker focused material around privacy.

However, Microsoft believes that consumer education is most effective when companies, consumer groups and government can work cooperatively. This is why we often support educational initiatives and work in partnership with consumer advocates and government agencies to develop educational materials on consumer privacy and data security, such as:

- GetNetWise. Microsoft supports this public education organization and website (www.getnetwise.org), which offers Internet users resources for making informed decisions about safer Internet use.

- Internet Keep Safe Coalition (www.ikeepsafe.org). Microsoft is a part of this partnership of governors, attorneys general, public health and educational professionals, law enforcement, and industry leaders working together for the health and safety of youth online.

- National Cyber Security Alliance (NCSA). Microsoft is part of this nonprofit public-private partnership that offers online safety and security information to the public on the http://www.staysafeonline.org website and through educational efforts such as National Cyber Security Awareness Month.

- Stop. Think. Connect (http://safetyandsecuritymessaging.org). Microsoft and a host of other organizations support this online safety campaign that promotes greater awareness and safer behavior on the web.

Finally, we applaud the Commission for its work in educating both consumers and businesses about the importance of protecting privacy and the best practices for doing so. For example, OnGuard Online[26] (which Microsoft helped the FTC develop) provides consumers practical advice in an easy-to-use and interactive format. And Admongo[27] is another innovative educational tool that helps children learn more about online advertising. Businesses also have benefited from the many guidance documents that the FTC provides online, ranging from children's to health privacy. The FTC is in a unique position to reach all consumers and businesses, and these materials are all important steps to helping ensure that consumers' privacy is protected.

## III. CONCLUSION

Microsoft appreciates the opportunity to comment on staff's preliminary report on consumer privacy and applauds the Commission's focus on this important set of issues. We hope that our comments prove helpful as the FTC continues to clarify the scope and application of the framework.

---

[26] *See* http://www.onguardonline.gov/ and http://www.ftc.gov/opa/2005/09/onguardonline.shtm.

[27] *See* http://www.admongo.gov/.

Please do not hesitate to contact me if you have any questions about our comments. Microsoft looks forward to working with you and other stakeholders to continue a productive dialogue aimed at providing sound guidance to businesses and helping to ensure that consumers' privacy interests are protected as technology continues to advance.

Sincerely,

Michael D. Hintze
Associate General Counsel
Microsoft Corporation