STATEMENT OF ERICH ANDERSEN
DEPUTY GENERAL COUNSEL
MICROSOFT CORPORATION

BEFORE THE
COMMITTEE ON COMMERCE, SCIENCE & TRANSPORTATION
UNITED STATES SENATE

HEARING ON THE STATE OF ONLINE CONSUMER PRIVACY

"THE NEED FOR A COMPREHENSIVE APPROACH TO PROTECTING CONSUMER PRIVACY"

MARCH 16, 2011

Chairman Rockefeller, Ranking Member Hutchison, and honorable Members of the Committee, my name is Erich Andersen, and I am Deputy General Counsel of Microsoft's Windows Division. Thank you for the opportunity to share Microsoft's views on an issue that needs the attention of Congress and the work of this Committee: the adoption of meaningful privacy legislation that protects individuals' privacy while complementing technological and industry-based measures and promoting continued innovation. We appreciate the leadership that the Committee has shown on this issue, and we are committed to working collaboratively with you, the Federal Trade Commission, the Department of Commerce, consumer groups, and other stakeholders to achieve this important balance.

In my role for the Windows Division, I have worked with our software team to develop privacy-enhancing features and tools for Windows and Internet Explorer. We have teams working on similar efforts throughout Microsoft – for instance, in the Bing search team, the online advertising division, the Xbox group, and our cloud computing group. Our goal across Microsoft is to build trust with consumers by giving them the tools they want to make them productive and enrich their computing experience. Privacy is a critical component of earning and maintaining that trust. In all of our service offerings, we strive to be transparent about our privacy practices, offer meaningful privacy choices, and protect the security of the data we store.

The multiple contexts in which we engage with consumers give us a unique perspective on the privacy discussion. For example, as a website operator, an ad network, and a browser manufacturer, we have a deep understanding of the roles that different participants in the digital ecosystem play in safeguarding consumer privacy. Also, based on our longstanding involvement in the privacy debate, we recognize that the combined efforts of industry and

government are required to effectively balance the need to protect consumers' privacy interests and promote innovation. In light of our experience, we recommend a multi-pronged approach that includes legislation, industry self-regulation, technology tools, and consumer education.

Today, I will explain why we believe that each of these four elements is important for protecting consumer privacy, and I will highlight steps that Microsoft has taken in each area. But first I would like to start with a discussion of how technology has reshaped consumers' engagement online and their privacy expectations.

I. Protecting Privacy While Enabling Innovation

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 web-based services have brought tremendous social and economic benefits. At the same time, however, technology has fundamentally redefined how, where, and by whom data is collected, used, and shared. The challenge that industry and government must address together is how to best protect consumers' privacy while enabling businesses to develop a wide range of innovative products and services.

Consider, for example, online advertising. Online advertising is the fuel that powers the Internet and drives the digital economy. Over $25 billion was spent on online advertising in 2010.[1] Millions of websites are able to offer their content and services for free because of the revenue they derive from advertising online. For small- and medium-sized businesses in particular, online advertising has created new opportunities to inform consumers about their products and services. One study estimates that the advertising-supported Internet

---

[1] Kristen Schweizer, *U.S. Web Advertising Exceeds Newspaper Print Ads in 2010, eMarketer Says*, BLOOMBERG (Dec. 20, 2010), http://www.bloomberg.com/news/2010-12-20/u-s-web-ads-exceed-newspaper-print-ads-in-2010-emarketer-says.html.

ecosystem is responsible for creating 3.1 million American jobs, and that the dollar value of these wages totals approximately $300 billion.[2] Consumers also benefit – not only because online advertising enables the free services and content they enjoy, but because the ads they see are more likely to be relevant. Simply put, the richness and vibrancy of the modern Internet experience is due in large part to the success of online advertising.

The collection of data to serve ads on the Internet also has important privacy implications. When Justice Louis Brandeis famously defined privacy as "the right to be let alone" in 1890,[3] he could not have foreseen how technology would revolutionize our world. An individual planning a trip to Boston can now go online to compare airfares, book a hotel room, map out restaurant recommendations that are convenient to her itinerary, and poll her network of friends for suggestions about things to do during her trip. Every day, people generate billions of page views, transactions, downloads, and search queries – a mountain of data, across a myriad of different devices, that reveals valuable information about users' interests. As one of Microsoft's senior executives recently recognized, industry can and must do better in addressing the fact that consumers often do not understand the ways in which their data is bought, sold, bartered, exchanged, traded, and used.[4]

In the digital era, privacy is no longer about being "let alone." Privacy is about knowing what data is being collected and what is happening to it, having choices about how it is collected and used, and being confident that it is secure. These three principles—transparency,

---

[2] Hamilton Consultants, Inc., *Economic Value of the Advertising-Supported Internet Ecosystem* 4 (June 20, 2009), http://www.iab.net/media/file/Economic-Value-Report.pdf.

[3] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[4] *See* Emily Steel, *Microsoft Executive Urges Online Ad Industry to Police Itself*, WALL ST. J. DIGITS BLOG (Feb. 28, 2011, 6:28 PM), http://blogs.wsj.com/digits/2011/02/28/microsoft-executive-urges-online-ad-industry-to-police-itself/ (referencing comments by Rik van der Kooi, corporate vice president of Microsoft's Advertiser & Publisher Solutions group, at the annual leadership meeting of the Interactive Advertising Bureau).

control, and security—underpin Microsoft's approach to privacy. They are also essential components of the thoughtful privacy frameworks recently advanced by the Federal Trade Commission ("FTC") and the Department of Commerce.[5] We believe that the principles of transparency, control, and security should inform legislative, self-regulatory, technological, and educational initiatives to safeguard consumer privacy.

II. A Role for Congress and Comprehensive Privacy Legislation

As we focus on what can be improved, it is important to note that in the past year, significant progress has been made toward protecting individuals' privacy: technological solutions to empower consumers to control their personal information are now widely available, consumers are much more educated about the nature and scope of privacy risks, enforcement actions have been taken by the FTC, and legitimate industry practices are becoming better and more consistent. Federal legislation can be an effective *complement* to this strategy, providing an additional layer of protection for consumers and another tool for enforcement officials.

Historically, Congress has played an active role in protecting consumers online. Beginning in the late 1990s, Congress passed laws aimed at specific online harms and revised existing laws to account for the evolving ways in which technology was being used to collect, use, and share personal information. Examples include the Children's Online Privacy Protection Act of 1998, the privacy and security provisions for financial information in 1999's Gramm-Leach-Bliley Act, the CAN-SPAM Act of 2003, and the breach notification provisions for protected health information that were included in 2009's Health Information Technology for

---

[5] *See generally* Fed. Trade Comm'n, Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010) [hereinafter FTC Staff Report]; Internet Policy Task Force, Dep't of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010) [hereinafter Commerce Report]. As we noted in comments filed with the FTC and the Commerce Department, we applaud the Commission's and Department's efforts to develop a robust privacy framework that will withstand rapid technological advances while fostering innovation.

Economic and Clinical Health Act. Congress (and this Committee in particular) has also scrutinized important privacy-related issues such as online advertising, data security and breach notification, privacy in connection with broadband providers, spyware, and children's online safety.

Although the progress that has been made is notable and should not be overlooked, our view since 2005 has been that Congress should take the next step and enact comprehensive federal privacy legislation. One of the key problems with the current sectoral approach to privacy regulations is that it makes compliance a complex and costly task for many organizations. According to one estimate, by 2009 there were over 300 federal and state laws relating to privacy.[6] The sector-specific approach also creates confusion among consumers, and can result in gaps in the law for emerging sectors or business models.

What industry needs is federal privacy legislation that sets forth baseline privacy protections for transparency, consumer control, and security that are not specific to any one technology, industry, or business model. Privacy protections that apply across sectors would provide consistent baseline protections for consumers, and simplify compliance for businesses that increasingly operate across those sectors. Baseline privacy protections would also promote accountability by ensuring that all businesses use, store, and share commercial data in responsible ways, while still encouraging companies to compete on the basis of more robust privacy practices. In addition, legislation would create legal certainty by preempting state laws that are inconsistent with federal policy.

---

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

Microsoft is pleased to see that members in both chambers of Congress are taking up the issue of comprehensive privacy legislation in the current congressional session, and we also find it encouraging that some of these initiatives appear to have early bipartisan support. As these proposals advance through the legislative process, we note that any privacy legislation should be crafted with two goals in mind. First, the legislation must protect consumers' privacy and data security while enabling innovation and facilitating the productivity and cost-efficiency offered by new business models and computing paradigms. Second, the legislation should create privacy protections that can withstand the rapid pace of technological change so that consumer data is protected not only today, but also in the decades to come.

To achieve these two ends, any proposed legislation should be tested against certain fundamental criteria, among them:

- Flexibility. The legislation should permit businesses to adapt their policies and practices to match the contexts in which consumer data is used and shared and be sufficiently flexible to allow technological innovation to flourish.

- Certainty. The legislation should provide businesses with certainty about whether their privacy policies and practices comply with legal requirements.

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

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

- Focus on substantive outcomes. Instead of imposing prescriptive rules that may be of limited effect or that may burden businesses without yielding commensurate privacy benefits, the legislation should set privacy goals based on criteria established in current public policy, then permit 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.

We look forward to continuing to work with this Committee to craft legislation that meets these criteria.

III. A Role for Industry Self-Regulation and Best Practices

Legislation, while important, is only part of the solution. Legislation is an appropriate vehicle for setting baseline standards, but it must work in conjunction with industry self-regulation and best practices, technology solutions, and consumer education.

Industry self-regulation is a useful complement to legislation for two reasons. First, self-regulatory efforts can easily be tailored to the particular context in which data about individuals is collected and used. Consumers have different privacy expectations depending on whether they are interacting with retailers, application developers, social media platforms, search engines, Internet service providers, publishers, advertisers, ad networks, or data exchanges. Effective privacy protections should take into account consumers' reasonable expectations of privacy, and industry self-regulation offers a flexible tool for doing so. Second, self-regulatory efforts are generally well-positioned to keep pace with evolving technologies and business models. There is no question that technology, business models, and consumer adoption of online services will continue to change – and change rapidly. 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 2003 Facebook was just an idea in the mind of a Harvard undergraduate, but today there are companies whose entire business model is built around developing applications for Facebook and other social media platforms.

Given the complex and dynamic nature of the online ecosystem, crafting workable solutions requires engagement from multiple stakeholders. Microsoft has a history of working collaboratively with other companies to develop appropriate solutions that build on the

principles of transparency, control, and security. For example, Microsoft is a strong supporter of the Self-Regulatory Program for Online Behavioral Advertising, which includes an educational website where consumers can learn about online advertising and choose not to have their information used for behavioral advertising. Additionally, data security is one of the focal points of the Program: participating organizations must agree to provide appropriate security for, and limit their retention of, data collected and used for behavioral advertising. In our multiple roles as a browser manufacturer, ad network, and website operator, we are coordinating with the Interactive Advertising Bureau and other participants in the Self-Regulatory Program to ensure that this important initiative is effective, enforceable, and broadly accepted. Consistent with our commitment to responsible industry leadership, we are also working at the World Wide Web Consortium, the standards-setting body for the Web, to develop an industry consensus about technical standards that can implemented across browsers to enable common tools for consumers to block tracking activities by third parties.

Transparency, control, and security are also essential concepts in Microsoft's Privacy Guidelines for Developing Software Products and Services, which are based on our internal privacy standards. We make these standards publicly available at http://www.microsoft.com/privacy for other organizations to use when developing and guiding 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.

IV. A Role for Technology Solutions

As a technology company, we naturally believe that technology has a key role to play in protecting consumer privacy. To ensure that we engineer privacy into our products from the outset and consider privacy issues throughout the project lifecycle, we have implemented internal policies and procedures that advance key principles such as transparency, control, and

security.[7] For example, in individual business groups such as Windows, Office, and Xbox, we have a three-tier system of privacy managers, privacy leads, and privacy champs who help make sure that our products and services comply with our standards and applicable privacy laws. We also have a dedicated Trustworthy Computing team that works with business groups across the company to ensure that their products and services adhere to Microsoft's security and privacy policies. Although my colleagues in other divisions would be delighted to provide you with details about our initiatives for Bing, Kinect, and other products and services, I want to focus on our industry-leading browser, Microsoft's Internet Explorer.

Internet Explorer has really been a pioneering technology for protecting consumer privacy online. It was the first browser to introduce InPrivate Browsing, a feature that prevents a consumer's browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser, thereby leaving virtually no evidence of the consumer's browsing history. Another feature in Internet Explorer 8, InPrivate Filtering, watches for third-party content that appears with high frequency across websites from companies that may be engaged in tracking activities, while still allowing consumers to view the content on the sites they've chosen to visit.

The InPrivate features were breakthroughs, but what I would like to highlight today is that Microsoft was the first of the major browser manufacturers to respond to the FTC's recent call for a persistent, browser-based "Do Not Track" mechanism.[8] The version of our

---

[7] Both the FTC's proposed framework and legislation currently moving through Congress recognize the importance of a robust privacy by design program. We support these efforts to encourage industry to incorporate privacy protections into their data practices and to develop comprehensive privacy programs.

[8] *See* FTC Staff Report 66 ("Commission staff supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as 'Do Not Track.' . . . The most practical method of providing uniform choice for online behavioral advertising would likely involve placing a setting similar (continued...)

browser that is being released this week, Internet Explorer 9, will offer an innovative new feature, "Tracking Protection," that allows consumers to decide which sites can receive their data and filters content from sites identified as privacy threats. Users will be able to create or download Tracking Protection Lists that identify websites which are, in the view of the list creator, trustworthy or untrustworthy. If a site is listed as a "do not track" site on a Tracking Protection List, Internet Explorer 9 will block third-party content from that site, unless the user visits the site directly by clicking on a link or typing its web address. By limiting "calls" to third-party websites, Internet Explorer 9 limits the information these third-party sites can collect – without relying on the third-party sites to read, interpret, and honor a do-not-track signal. 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.

The Tracking Protection feature is highly customizable and can be adapted to specific user preferences because anyone on the Web (including consumer groups and privacy advocates, enterprises, security firms, and consumers) will be able to create and publish Tracking Protection Lists – they are simply files that can be uploaded to a website and made available to others via a link. Tracking Protection also supports user control: consumers can create or subscribe to more than one list if they wish, they can subscribe and unsubscribe to lists as they see fit, and a decision to subscribe to a list or lists will enable Tracking Protection across all browsing sessions until the consumer chooses to turn it off. Finally, Tracking Protection was designed with security in mind: because the Web evolves over time and third parties might migrate to new domain names, Internet Explorer 9 will automatically check for updates to a

---

to a persistent cookie 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.").

consumer's lists on a regular basis, helping ensure that the lists address the latest privacy and security threats.

V. A Role for Consumer Education

We agree with the FTC and the Commerce Department that there is a need for greater consumer education to increase consumer understanding of data practices and their privacy implications.[9] At Microsoft, we recognize that it is crucial to engage and educate consumers, to give them a voice and build a bridge to mutual understanding and benefit. That is why we provide consumers with clear information about our own practices and, where appropriate, offer choices about what data will be collected and how it will be used.

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, including the concepts of purpose specification and use limitation. Moreover, as noted above, we offer consumers easy ways to learn about online behavioral advertising and the privacy practices associated with the particular advertisements they receive, and to opt out of behavioral advertising if they so choose.

We have also partnered with consumer advocates and government agencies to develop educational materials on consumer privacy and data security, such as:

- 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.

---

[9] *See* FTC Staff Report 78–79; Commerce Report 31–36.

- 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.

- 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.

We believe that such initiatives are important for ensuring that consumers understand the importance of protecting their privacy and security online, and are equipped with the tools to do so.

VI. Conclusion

Thank you for extending us an invitation to share our experience and recommendations with you. We commend the Committee for holding this hearing today, and we look forward to working with you to craft meaningful privacy protections that provide transparency, control, and security in a way that honors individuals' privacy expectations, complements existing technological and industry-based solutions, and promotes innovation.