



Lead more



Microsoft and Data Privacy

Helping to Protect Personal Information
in the Digital Era

Microsoft

Agenda

- Online Privacy and Data Security: An Evolving Landscape
- Privacy Fundamentals at Microsoft
- Protecting Individual Privacy and Personal Data
- Helping Organizations Manage and Protect Personal Information
- Advancing Privacy Leadership and Collaboration

Online Privacy and Data Security: An Evolving Landscape

As a big company, we've got to lead on privacy.... We have a responsibility, all of us, not just to socially respect the user, but to build the technology that will protect the anonymity, the privacy, the security of what I say, who I say it to, where I go, what's important to me.

www.microsoft.com/presspass/exec/steve/2010/03-04Cloud.mspx - Microsoft CEO Steve Ballmer

Online Privacy and Data Security: An Evolving Landscape

- With the growth of data storage, access, and exchange via the Web, individuals' personal information has become the new currency of crime. Identity thieves are using spyware, phishing scams, and other illicit methods to steal billions of dollars a year through fraudulent financial transactions.
- Organizations that collect, store, and manage people's personal information are also vulnerable to theft or loss of data, which can lead to significant financial harm and damage to their reputation. Such data breaches are increasingly problematic for businesses and government, and they are undermining public trust in e-commerce and online services. Increasingly, people are wary of new technologies and business models that might lead to the misuse or abuse of their personal information.
- Maintaining and building public confidence in the ability of governments and business organizations to responsibly manage and protect individuals' data is essential if the Internet and related technologies are to reach their full potential.

Privacy Fundamentals at Microsoft

Microsoft develops many technologies that enable greater access to and use of information, and we understand that respect for privacy is essential to enabling a more trustworthy computing environment. We believe that individuals should have control over their personal information and that organizations should be responsible and accountable for how they collect, use, and protect this information.

Microsoft Privacy Principles

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

Protecting Individual Privacy and Personal Data



Microsoft backs its online services with strong data protection tools and clear privacy policies.

Search Privacy Practices Chart

January 2010

Microsoft



De-identification: Search queries stored separately from any account information that could directly identify an individual (such as name and address), linkable to each other and PC, with technical protections in place to prevent the data from being connected to personally identifying information.

Full IP Address Removed: Deletion of the entire IP Addresses associated with search queries.

Complete anonymization: Complete removal of full IP address and cross-session identifiers.

Protecting Individual Privacy and Personal Data:

- As part of Microsoft's privacy safeguards for user information gathered through Bing, search terms are stored separately from information that could personally and directly identify an individual. This helps protect against unauthorized correlation of these details by either Microsoft or third parties. Search-related data is maintained only as long as necessary for us to deliver and improve our services, after which we make the data anonymous by deleting all cross-session identifiers. In early 2010, we announced that we would enhance our existing search anonymization processes by deleting the entire IP address from search queries after six months. This step will provide even stronger privacy protections for Bing users.
<http://microsoftontheissues.com/cs/blogs/mscorp/archive/2010/01/18/microsoft-advances-search-privacy-with-bing.aspx>
- Our Online Privacy Statement includes a supplement (<http://privacy.microsoft.com/en-us/bing.mspx>) that details how Bing retains information about search terms that users enter and the results they click on in order to provide an easy way for users to revisit those sites and searches. It also provides a link to simple steps that show how individuals can turn off or clear their search history.

Online Advertising

- At Microsoft, we believe that individual choice and control are essential to crafting a successful advertising business model that brings value to all stakeholders. We are working to provide these capabilities through our strong internal business practices and support for uniformly high standards of industry self-regulation.
- Microsoft selects relevant ads for individual users based on data that does not personally and directly identify the user. One way we achieve this important privacy protection is through the use of a pseudonymous identifier, which takes the form of a cookie placed on the user's PC. This allows the Microsoft adCenter platform to attach details about the user's interests and demographic information to a particular cookie without correlating it with data that could be used to directly identify that individual.
- Within the Microsoft Online Privacy Statement, our online advertising policy clearly spells out the types of personal information we collect and their potential uses. Consistent with our principle of providing customers with the ability to control how their information is used, we offer several ways for individuals to opt out of online advertising. For example, an opt-out page linked from the Online Privacy Statement allows people to easily opt to not receive ads based on usage data—not only across Microsoft's own Web sites but also across other sites where we deliver ads. Further, users can decide to make this opt-out choice persistent and —roamablell—applicable to any computer that they log onto using a Windows Live ID.
- Microsoft also collaborates with governments, public interest groups, self-regulatory bodies, and Internet companies around the world to establish and strengthen best practices regarding user notice, control, data anonymization, and related online advertising privacy protections. In the United States, we recommended that the Federal Trade Commission (FTC) adopt a tiered approach that imposes increasingly strict privacy obligations based on the type of online advertising activity, behavioral or otherwise, that an organization pursues and the kind of personal information being collected. Similar collaborative efforts are under way with governments in the European Union, the Asia-Pacific region, and elsewhere.
- In addition, Microsoft subscribes to the Self-Regulatory Principles for Online Behavioral Advertising (www.iab.net/media/file/ven-principles-07-01-09.pdf), which we helped to develop in concert with a broad coalition of industry groups, advertisers, Web publishers, and ad networks.

Software Tools and Features

Individual privacy and data protection are paramount in the design, development, and deployment of all Microsoft software products and services. We provide a range of technology tools and features designed to help individuals do the following:

Control their personal information. Assurance of privacy on the Web requires clear disclosure and choice for individuals. Disclosure includes informing people in plain language about the data being collected and how it will be used. Choice involves giving them the tools to control and protect their own data.

For example, the InPrivate Browsing and InPrivate Filtering options in Internet Explorer® 8 give individuals greater control over details about their online activities. InPrivate Browsing helps prevent users' browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser, thereby leaving virtually no evidence of their browsing or search history. InPrivate Filtering helps individuals control the elements—such as maps, ads, scripts, or images—that third-party Web sites can potentially use to track their browsing activity. To learn more about privacy features in Internet Explorer 8, go to www.microsoft.com/windows/internet-explorer/features/safer.aspx.

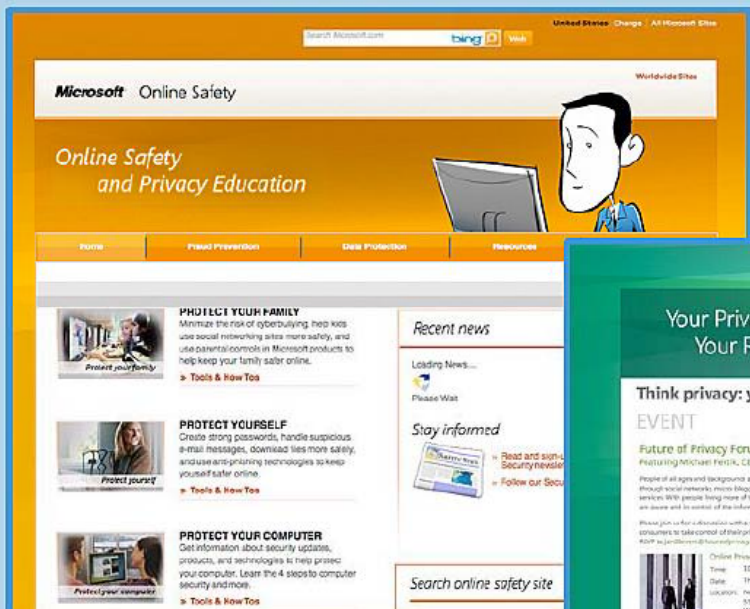
Block unwanted communications and protect themselves from harm. The widespread gathering and sharing of information over the Internet can expose people to intrusive contact from overly aggressive marketers as well as potentially harmful scams by cybercriminals seeking to steal personal data. Microsoft is investing significant resources to create a trustworthy environment in which computers provide layered defenses against malicious code, phishing attacks, spam, and other threats to individual privacy.

The SmartScreen Filter (www.microsoft.com/security/filters/smartscreen.aspx), part of Internet Explorer 8 and Microsoft's e-mail platforms, helps identify and block intrusive communications as well as dangerous online content by notifying people when they try to visit a Web site or download software that has been reported as unsafe. The Malicious Software Removal Tool (www.microsoft.com/security/malwareremove/default.aspx) looks for and removes the most prevalent malicious software families from PCs running Windows® 7, Windows Server® 2010, and several previous Microsoft operating systems. We also offer Microsoft Security Essentials (www.microsoft.com/security/products/mse.aspx), a free download that protects against viruses, spyware, and other malicious software.

Guidance and Education

For most people, weighing the many variables associated with protecting their privacy and information when using the Internet is a complex challenge. Microsoft has developed a worldwide education campaign that includes information and tools to help individuals protect themselves and their families, their PCs, and their personal information. Information about these efforts is available at www.microsoft.com/protect

We also provide free resources to educators and policymakers to help them create local or national privacy and Internet safety education programs.



Microsoft provides a wealth of resources designed to raise awareness about data privacy issues and help individuals protect their personal information online.



Helping Organizations Manage and Protect Personal Information



Technology Domains for Data Governance

Microsoft provides an array of enterprise products that are designed to help organizations strengthen the privacy and confidentiality of data as well as implement appropriate regulatory compliance measures across the following areas:

Secure Infrastructure: Technology that protects computers, storage devices, operating systems, applications, and the network against malicious software and hacker intrusions as well as rogue insiders.

Identity and Access Control: Identity and access management technologies that protect confidential information from unauthorized access while making it readily available to legitimate users.

Information Protection: Tools that deliver persistent protection of data from interception and viewing by unauthorized parties. Key capabilities include file and data classification, identity and access controls, data encryption, and rights management.

Auditing and Reporting: Capabilities that make it easier for the organization to comply with internal policies, government regulations, and consumer demands for better control over sensitive data. Microsoft solutions can help IT teams streamline systems management and monitoring, automate compliance controls, verify that system and data access controls are operating effectively, and identify suspicious or noncompliant activity.

www.microsoft.com/privacy/technologies.aspx

Advancing Privacy Leadership and Collaboration



End to End Trust

Privacy protection is an important part of End to End Trust—Microsoft's vision for achieving a safer, more trusted Internet by enabling users to make more effective choices about whom and what to trust online. We are working to realize this vision through our internal initiatives and through industry collaboration in three key areas:

Security and privacy fundamentals. We continually focus on building more secure and privacy-enhanced software and services. These efforts include implementing and sharing our Security Development Lifecycle (<http://msdn.microsoft.com/en-us/library/ms995349.aspx>) and Privacy Guidelines for Developing Software Products and Services.

Technology innovations. We are committed to creating comprehensive security protections to build greater trust at each point in a digital transaction—including hardware, software, people, and data involved. This includes a robust digital online identity system that provides greater protection from fraud and abuse without compromising personal privacy.

Social, economic, political, and technological alignment. We collaborate with individuals, partners, industry, governments, and other important constituencies to help ensure that privacy-focused technology innovations are aligned with social, political, and economic considerations.

www.microsoft.com/mscorp/twc/endtoendtrust

Conclusion

Realizing the full potential of the Internet as a driver of economic and social benefits will require higher levels of trust, accountability, and security online. Adoption of new Internet products and services depends on users feeling confident that their personal data will be protected. Microsoft is strongly committed to strengthening individual and organizational privacy in the digital ecosystem through the following tools and measures:

- Rigorous corporate policies, principles, technical standards, and other measures that are systematically incorporated into the development of Microsoft's products and services to help ensure privacy and data protection**

- Easy-to-use software that allows individuals to more safely and confidently share their information online, along with practical tips for steering clear of threats**

- Enterprise-level technology tools and guidance for public- and private-sector organizations to help them more securely manage personal data and meet compliance requirements**

- Engagement with government, industry, law enforcement, and public-interest partners**

Microsoft believes that a trustworthy and privacy-assuring online ecosystem can be achieved through a combination of innovative technology, legislation, policies and practices, training, and guidance. Organizations, technology providers, governments, and privacy advocates must work together to make this a reality.

Microsoft®

Be What's Next.