



online privacy alliance

**An alliance of global companies & associations
committed to promoting privacy online.**

Privacy Guidelines

Companies

Acxiom
America Online, Inc.
Ameritech
Apple Computer
AT&T
Bank of America
Bell Atlantic
Cisco
Compaq
Dell
Disney
Dun & Bradstreet
eBay Inc.
Eastman Kodak, Co.
EDS
E-LOAN
Engage Technologies Inc.
Equifax
Ernst and Young
Experian
Ford
Gateway
GeoCities
Hewlett-Packard
IBM
InsWeb Corporation
KPMG
LEXIS-NEXIS
MatchLogic
MCI
Microsoft
Narrowline Inc.
NCR
NETCOM On-Line Communication Services,
Inc.
Netscape
Network Risk Management Services
NORTEL
Oracle
Preview Travel
PricewaterhouseCoopers
Procter & Gamble
Sun Microsystems
Time Warner Inc.
Unilever United States, Inc.
Viacom
ViewCall Canada, Inc.
WebConnect
Xerox
Yahoo!

Associations

American Advertising Federation
American Electronics Association
American Institute of Certified Public
Accountants
CASIE (CASIE is representing Association of
National Advertisers & American
Association of Advertising Agencies)
Association of Online Professionals
Computer Systems Policy Project (CSPP)
Council of Growing Companies
Direct Marketing Association
European-American Business Council
Individual Reference Services Group
Information Technology Association of America
Information Technology Industry Council
Interactive Travel Services Association (ITSA)
Internet Alliance
The Software Publishers Association
The United States Council for International
Business
The United States Chamber of Commerce

November 19, 1998



An alliance of global companies & associations
committed to promoting privacy online.

Mission Statement

The Online Privacy Alliance will lead and support self-regulatory initiatives that create an environment of trust and that foster the protection of individuals' privacy online and in electronic commerce.

The Alliance will:

- identify and advance effective online privacy policies across the private sector;
- support and foster the development and use of self-regulatory enforcement mechanisms and activities, as well as user empowerment technology tools, designed to protect individuals' privacy;
- support compliance with and strong enforcement of applicable laws and regulations;
- support and foster the development and use of practices and policies that protect the privacy of children;
- promote broad awareness of and participation in Alliance initiatives by businesses, non-profits, policy makers and consumers; and
- seek input and support for Alliance initiatives from consumer, business, academic, advocacy and other organizations that share its commitment to privacy protection.

Membership Pledge

As members of the Alliance:

- we endorse its mission;
- we commit ourselves to implement online privacy policies consistent with the Alliance's guidelines; and
- we commit ourselves to participate in effective and appropriate self-regulatory enforcement activities and mechanisms.



An alliance of global companies & associations
committed to promoting privacy online.

Guidelines for Online Privacy Policies

Upon joining the Online Privacy Alliance, each member organization agrees that its policies for protecting individually identifiable information in an online or electronic commerce environment will address at least the following elements, with customization and enhancement as appropriate to its own business or industry sector.

1. Adoption and Implementation of a Privacy Policy

An organization engaged in online activities or electronic commerce has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information. Organizations should also take steps that foster the adoption and implementation of effective online privacy policies by the organizations with which they interact; e.g., by sharing best practices with business partners.

2. Notice and Disclosure

An organization's privacy policy must be easy to find, read and understand. The policy must be available prior to or at the time that individually identifiable information is collected or requested.

The policy must state clearly: what information is being collected; the use of that information; possible third party distribution of that information; the choices available to an individual regarding collection, use and distribution of the collected information; a statement of the organization's commitment to data security; and what steps the organization takes to ensure data quality and access.

The policy should disclose the consequences, if any, of an individual's refusal to provide information. The policy should also include a clear statement of what accountability mechanism the organization uses, including how to contact the organization.

3. Choice/Consent

Individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them online may be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to opt out of such use. Additionally, in the vast majority of circumstances, where there is third party distribution of individually identifiable information, collected online from the individual, unrelated to the purpose for which it was collected, the individual should be given the opportunity to opt out.

Consent for such use or third party distribution may also be obtained through technological tools or opt-in.

4. Data Security

Organizations creating, maintaining, using or disseminating individually identifiable information should take appropriate measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse or alteration. They should take reasonable steps to assure that third parties to which they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect any transferred information.

5. Data Quality and Access

Organizations creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to assure that the data are accurate, complete and timely for the purposes for which they are to be used.

Organizations should establish appropriate processes or mechanisms so that inaccuracies in material individually identifiable information, such as account or contact information, may be corrected. These processes and mechanisms should be simple and easy to use, and provide assurance that inaccuracies have been corrected. Other procedures to assure data quality may include use of reliable sources and collection methods, reasonable and appropriate consumer access and correction, and protections against accidental or unauthorized alteration.

• • •

These guidelines are not intended to apply to proprietary, publicly available or public record information, nor to supersede obligations imposed by statute, regulation or legal process.

Other valuable resources available to Alliance members in the development of privacy policies include: the OECD's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"; the U.S. Department of Commerce's "Staff Discussion Paper of Privacy Self-Regulation"; and various industry association programs.



An alliance of global companies & associations
committed to promoting privacy online.

Principles for Children's Online Activities

The Members of the Online Privacy Alliance believe that the development of interactive online communications provides tremendous opportunities for children. At the same time, it presents unique challenges for protecting the privacy of young children. Children under 13 are special. Unlike adults, they may not be fully capable of understanding the consequences of giving out personal information online. However, children often understand how to navigate online far better than their parents do. Parents will not always have the knowledge, the ability or the opportunity to intervene in their children's choices about giving out personal information. Therefore, companies operating online must protect the privacy of children.

In connection with online activities of children under 13, the Alliance adopts the following principles.

Companies doing business online that operate sites that are directed at children under 13 or at which the age of visitors is known, must at those sites:

- Not collect online contact information from a child under 13 without prior parental consent or direct parental notification of the nature and intended use of this information, which shall include an opportunity for the parent to prevent use of the information and participation in the activity. This online contact information shall only be used to directly respond to the child's request and shall not be used to recontact the child for other purposes without prior parental consent.
- Not collect individually identifiable offline contact information from children under 13 without prior parental consent.
- Not distribute to third parties any individually identifiable information collected from a child under 13 without prior parental consent.
- Not give the ability to children under 13 to publicly post or otherwise distribute individually identifiable contact information without prior parental consent. Sites directed to children under 13 must take best efforts to prohibit a child from posting contact information.
- Not entice a child under 13 by the prospect of a special game, prize or other activity, to divulge more information than is needed to participate in that activity.



An alliance of global companies & associations
committed to promoting privacy online.

Effective Enforcement of Self-Regulation

Summary

Effective enforcement of online privacy policies is intended to assure an organization's compliance with its privacy policies for the collection, use and disclosure of personally identifiable information online and provide for consumer complaint resolution. Whether administered by a third-party privacy seal program, licensing program or a membership association, the effective enforcement of self-regulation requires: 1) verification and monitoring, 2) complaint resolution and 3) education and outreach. The Online Privacy Alliance believes the best way to create public trust is for organizations to alert consumers and other individuals to the organization's practices and procedures through participation in a program that has an easy to recognize symbol or seal.

Third-Party Enforcement Programs

Validation by an independent trusted third party that organizations are engaged in meaningful self-regulation of online privacy, may be necessary to grow consumer confidence. Such validation should be easily recognized by consumers, for example through the use of a seal or other symbol. The symbol or seal can be used to connote both compliance with privacy policies and an easy method for consumers to contact the seal provider. Thus, the Online Privacy Alliance supports third-party enforcement programs that award an identifiable symbol to signify to consumers that the owner or operator of a Web site, online service or other online area has adopted a privacy policy that includes the elements articulated by the Online Privacy Alliance, has put in place procedures to ensure compliance with those policies, and offers consumer complaint resolution.

Privacy Seal Program

Such a privacy seal program (hereinafter "the seal program") should implement mechanisms necessary to maintain objectivity and build legitimacy with consumers. The seal program should utilize a governing structure that solicits and considers input from the business community, consumer/advocacy organizations and academics in formulating its policies. The seal program should strive to create a consistent and predictable framework in implementing its procedures. The seal program should be independent and should endeavor to make receipt of the seal affordable for and available to all online businesses.

A seal program should include the following characteristics:

- **Ubiquity:** In order to minimize confusion and increase consumer confidence, efforts shall be taken to ensure ubiquitous adoption, and recognition of seals through branding efforts, including, for example, co-branding with corporations or associations.
- **Comprehensiveness:** A seal program should be flexible enough to address issues related to both sensitive and non-sensitive information.

- **Accessibility:** A seal should be easy for the user to locate, use and comprehend.
- **Affordability:** The cost and structure of a seal should encourage broad use and should not be prohibitive to small businesses. The cost of a seal will vary based on a number of factors, including the extent and complexity of review, size of the business, the amount and type of individually identifiable information collected, used and distributed, and other criteria.
- **Integrity:** A seal provider should be able to pursue all necessary avenues to maintain the integrity of the seal, including trademark enforcement actions.
- **Depth:** A seal provider should have the ability to handle the number and breadth of consumer inquiries and complaints about the potential violation of online privacy policies and should have an established set of mechanisms to address those inquiries and complaints.

Verification and Monitoring

A seal program must require that its participants adopt a privacy policy that comports with the principles endorsed by the Online Privacy Alliance. The scope of this requirement only applies to the participating organization and does not apply to the Web pages of affiliates or other Web pages linked to or from the participating organization's Web page. While these baseline principles should be standardized, individual policies accepted by the seal provider should allow for sector-specific variations. The seal program must then require that an organization put in place either self-assessment or accept the seal program's compliance review prior to awarding the seal.

If a self-assessment system is chosen, it must be pursuant to a rigorous, uniform, clearly articulated and publicly disclosed seal program methodology under which an organization would be asked to verify that its published privacy policy is accurate, comprehensive, prominently displayed, completely implemented and accessible; and that consumers are informed of the consumer complaint resolution mechanisms through which complaints are handled. A statement verifying the self-assessment should be signed by a corporate officer or some other authorized representative of the company. The self-assessment should then be reviewed by the seal program to assure compliance with the methodology. Specific criteria for when a company should improve the implementation of its self-assessment system, adopt further measures, or circumstances when a third-party review is required, should be part of the seal program's methodology for acceptable self-assessment.

Periodic reviews should be required by the seal program to ensure that those displaying the seal continue to abide by their privacy policies and that those policies continue to be consistent with its principles. These periodic reviews may include, but are not limited to, auditing, random reviews, use of "decoys" or use of technology tools as appropriate to ensure that sites are adhering to the articulated privacy policies.

In cases where there is evidence that the company is not abiding by its privacy policies, the seal provider should establish clear criteria for placing that company on probation or beginning procedures for the seal's revocation. The seal provider should establish clearly defined criteria for when and how a company's seal may be revoked. A company should be given notice and the opportunity to request outside review before its seal is revoked. Seal revocation should be a matter of public record. The seal provider must clearly state the grounds for revocation and establish a post-revocation appeals process. In addition to the above criteria, the seal provider should also strive to ensure the integrity of the seal by monitoring for misuse or misappropriation.

Consumer Complaint Resolution

An effective third-party enforcement mechanism must provide its participants and consumers a structure to resolve complaints and consequences for failure to do so. Thus, a seal program must define the scope of complaints subject to the complaint resolution process, have a system in place to address complaints, the necessary staff to handle the volume of complaints and the organizational depth to resolve them. The seal program must provide a variety of easy mechanisms to allow consumers to lodge complaints or ask questions. Seal recipients must agree to the complaint resolution procedure.

Under the complaint resolution system, consumers must first be required to seek redress for their complaints from the company they believed to have aggrieved them, before being granted access to the seal program's complaint resolution mechanism. Where complaints cannot be adequately resolved by the company, and where the consumer and company have exhausted good faith efforts to reach agreement, the company should be required to submit to a complaint resolution mechanism.

Complaint resolution outcomes must not be contrary to any existing legal obligations of the participating company. Failure of a company to agree with the outcome of the seal program's complaint resolution should result in previously identified consequences to the company. Notwithstanding the complaint resolution process, the consumer, the company and the seal provider may pursue other available legal recourse.

Education and Outreach

A seal program must develop and implement policies to educate consumers and business about online privacy.

A seal program must develop and implement policies to encourage awareness of the program and online privacy issues with both consumers and businesses. Such techniques shall include: publicity for participating companies, public disclosure of material non-compliance or seal revocation, periodic publication of the results of the monitoring and review procedures, or referral of non-complying companies to the appropriate government agencies.



An alliance of global companies & associations
committed to promoting privacy online.

Online Privacy Alliance Association Policy

An association that joins the Online Privacy Alliance agrees to:

- endorse the Alliance mission statement, including: 1) adopting and posting privacy guidelines consistent with the Alliance's guidelines and appropriate to the association's membership; and 2) participating in self-regulatory enforcement mechanisms appropriate to the association's online activities;
- encourage its members to adopt privacy guidelines consistent with the Alliance's guidelines and appropriate to their industry's sector, and to implement appropriate self-regulatory mechanisms; and
- actively participate in the Alliance's business outreach and consumer education programs.

An association also may administer a seal or other third-party self-regulatory enforcement program at its discretion.