



online privacy alliance

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

Committed Organizations

Companies

Acxiom
America Online, Inc.
Apple Computer
AT&T
Bay Networks
Bell Atlantic
Cisco
Compaq
Dell
Disney
Dun & Bradstreet
Eastman Kodak, Co.
eBay Inc.
EDS
E-LOAN
Equifax
Ernst and Young
Experian
Ford
Hewlett-Packard
IBM
LEXIS-NEXIS
Lucent Technologies
MatchLogic
MCI
Microsoft
Narrowline Inc.
NationsBank
NCR
NETCOM On-Line
Communication Services, Inc.
Netscape
Oracle
Preview Travel
Price Waterhouse
Procter & Gamble
Sun Microsystems
Time Warner Inc.
Viacom
Xerox

Associations

American Advertising Federation
American Electronics Association
CASIE (representing Association of
National Advertisers & American
Association of Advertising
Agencies)
Direct Marketing Association
European-American Business
Council
Individual Reference Services Group
Information Industry Association
Information Technology Association
of America
Information Technology Industry
Council
Internet Alliance
The United States Chamber of
Commerce
The United States Council for
International Business

June 22, 1998

The Internet is poised to become an explosive economic growth opportunity that will redefine global commerce in the information age. That growth cannot and will not occur without consumer confidence. Privacy is one of the cornerstones of consumer confidence in the Internet.

Over the past several months numerous companies and associations have worked to create policies and practices that can make privacy a reality for everyone on the Internet. These companies and associations, the Online Privacy Alliance, are pleased to release the attached documents. First is the Mission Statement describing the goals of the Online Privacy Alliance, second are the Guidelines for Privacy Policies that will be adopted by all Online Privacy Alliance members, third are the Principles for Children's Online Activities, and fourth is a Statement on Enforcement of Self-Regulation.

The Online Privacy Alliance has worked diligently to come up with policies that can be applied across many industry sectors. Although it is not always easy to reach agreement in such a diverse group, when the agreement is forged everyone has a clear understanding of the responsibilities they are agreeing to undertake. These guidelines, principles and statements reflect not only a deep commitment to online privacy, but also new policies which the Online Privacy Alliance members support. First, the Online Privacy Alliance believes that when there is use or distribution of individually identifiable information for purposes unrelated to that for which it was collected, individuals should be given the opportunity to opt out of such unrelated use or distribution. Second, the Online Privacy Alliance members believe that sites targeted at children under 13 should not engage in the collection and maintenance of information from children without prior parental consent. Finally, the Online Privacy Alliance members believe that self-regulation requires robust enforcement and they are committed to ensuring such.

These documents reflect a beginning. The Online Privacy Alliance members are committed to continuing their work on these issues so that privacy can be a reality for everyone on the Internet. It has been a pleasure working with this group and I look forward to continuing to work with the Online Privacy Alliance to build consumer confidence in the Internet.



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.

Statement on Enforcement of Self-Regulation

The members of the Online Privacy Alliance believe that the cornerstone of effective self-regulation for online privacy is robust and ubiquitous enforcement of such self-regulation. Accountability for effective business practices regarding the collection, use, and distribution of individually identifiable information is an essential aspect of online privacy protection. We believe that both the private sector and the government have responsibility to enforce self-regulation. For example, in the private sector, TRUSTe and BBBOnLine have expanded or launched third party privacy seal programs and we believe such programs are essential to building consumer confidence in online privacy. In addition, many companies and associations are implementing self-administered compliance and enforcement programs. In the government, the Federal Trade Commission and the state attorneys general have the authority to prosecute organizations who post deceptive privacy policies, and we believe they should do so.

To be effective, private sector-based self-regulatory enforcement regimes should identify the appropriate mechanisms to ensure compliance (enforcement) and appropriate means of response to consumer complaints (redress). The type of enforcement necessary to protect privacy online will vary by industry sector. For example, sensitive information may require the highest levels of objective assurance that the data is protected.

Mechanisms to ensure compliance include, but are not limited to: making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association; ongoing assessments or audits to verify an organization's compliance with its stated policy; or validation that organizations have adopted and comply with a stated code. Appropriate means of individual redress may include any variety of mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed.

Any effective private sector self-regulatory enforcement mechanism must include the following elements:

- an ongoing assessment procedure for determining whether companies comply with their posted privacy policies that may include periodic public disclosure of the assessment methodology and results;
- accessible and responsive dispute resolution opportunities for individuals who believe that an organization has not collected, used or distributed their individually identifiable information in accordance with the organization's published privacy policy; and
- educational outreach to consumers and businesses regarding the importance of addressing individuals' privacy concerns.

The Online Privacy Alliance is working with groups who are interested in creating or expanding third party enforcement mechanisms. We are also working with organizations and associations to determine the necessary elements of self-administered enforcement programs. We also will explore the role of governments in enforcing self-regulation. We will release our specific recommendations for effective enforcement of self-regulation by September 15, 1998.