



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

Submitted by Christine Varney, cvarney@hhlaw.com

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.

###

The guidelines above are supplemented by:

The OPA Statement on "Effective Enforcement of Self Regulation," and
The OPA Statement regarding "Web Publisher Treatment of Network Advertisers"

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.