



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

Note: The following paper on aspects of "choice" is prepared for the Internet Caucus Advisory Committee's 2001 Privacy Briefing Book on the "Policy of Choice." It contains excerpts from the Online Privacy Alliance's "Privacy Guidelines Commentary" that can be read in its entirety, along with the OPA's "Guidelines for Online Privacy Policies," at <http://www.privacyalliance.org/resources/> .

Privacy Guidelines Commentary

November 19, 1998

ONLINE PRIVACY ALLIANCE

Commentary to the Mission Statement and Guidelines

INTRODUCTION

1. This commentary is intended to serve as an introduction to the Alliance's Mission Statement and Guidelines as well and to serve as an interpretive tool, which will assist Alliance Members and others to establish and refine on-line privacy programs internally and in working with third parties to develop enforcement programs. This document attempts to reflect the thoughts of the drafters of the Guidelines, their areas of disagreement, and the compromises they have reached in their final product. ...

PRINCIPLES FOR CHILDREN'S ON-LINE ACTIVITIES

40. In enunciating these principles, the Online Privacy Alliance has more clearly articulated principles of protection of children than has ever been done before. The Principles are based on two developmental assumptions and require parental consent whenever possible. The first developmental assumption is that children 12 and younger, or under the age of 13, are assumed not to know the potential consequences and dangers of disclosing personal information about themselves in a public forum, or to a commercial website. Consequently, collecting off-line contact information gathered from children requires the prior consent of a parent while collecting on-line contact information requires parental involvement. The age of 13 was not a random choice, but an age referred to in conferences at the Department of Commerce and in other forums by knowledgeable childhood development experts as the usual end of the age of innocence, when children learn that being untruthful about their age provides them access to forbidden fruit.

41. These principles apply in two special circumstances: where sites are intended to attract children under 13, and sites where the age of visitors is known, such as when the information gathered includes age. Those sites must follow the principles to obtain prior parental consent for carrying on certain activities, which are discussed below. Presumably, companies intending to attract children below the age of 13 will know their target audience's age, and provide the necessary mechanisms to comply with these principles. Similarly, when a site requests age information and a registrant answers that he or she is 12 or under, the site will automatically exclude the

child from being able to provide further personal information until the principles are complied with.

42. The first principle applies to the collection of **on-line** contact information by the site, that is, an E-mail address. A site doing this must either get a parent's consent or obtain, presumably from the child, a means of notifying the parent of the nature and intended use of the contact information, such as to E-mail the child notices of new events or features on the site. This notice to the parent must provide an opportunity to prevent use of the information or participation in the activity. This requirement might be met by providing E-mail notices that clearly explain how the parent can do this, such as by replying to the message and inserting one word in the body of the reply, such as "unsubscribe," as is done with listservs and other automatic broadcast subscription services.

43. This first principle represents the balance Alliance Members were able to strike between the desire to obtain that consent and the realities of the Internet. There is no way for a website to verify that someone identified by the child as a parent is indeed their parent. Because of this uncertainty, the use of this on-line contact information is restricted. For example, on-line contact information may be used to respond to a child's request, such as to receive a password, or to be told of new developments on the site, or to obtain parental consent. The site may not use the information to contact the child for other purposes, such as marketing, without the parent's consent.

44. Prior parental consent, as opposed to notification, must be obtained by a website when off-line contact information is gathered, such as a telephone number or home address, possibly even the name of a child's school; or when individually identifiable information about the child, including an E-mail address, is to be transferred to third parties, regardless of the purpose for which will be used; or the site permits a child to post or publicly distribute his or her individual contact information (such as an E-mail address). Sites that are designed to attract children under 13 must attempt to prohibit a child from posting contact information. Presumably, this means that the bulletin board or chat room will have a monitor to prevent this, or postings could be delayed until reviewed by an adult or technological means could be employed.

45. The principles are silent on how the parent's consent shall be obtained. Experience will demonstrate the best and safest practice in this regard. Given that this is an on-line medium, the first area of experimentation might involve eliciting the parent's E-mail address from the child. Other possibilities involve inviting the child to request a parent to write or telephone, or perhaps immediately participate in the child's registration at a site. One solution that would not be acceptable would be to elicit from the child the parent's off-line address or phone number, as this might be used to identify the child's off-site contact information.

ANNEX I

ELEMENTS OF EFFECTIVE SELF-REGULATION

FOR PROTECTION OF PRIVACY

As set forth in *A Framework for Global Electronic Commerce*, the Clinton administration supports private-sector efforts to implement meaningful, consumer-friendly, self-regulatory regimes to protect privacy. To be meaningful, self-regulation must do more than articulate broad policies or Guidelines. Effective self-regulation involves substantive rules, as well as the means to ensure that consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when injuries result from noncompliance. This paper discusses the elements of effective self-regulatory regimes -- elements that incorporate principles of fair information practices with enforcement mechanisms that ensure compliance with those practices.

A. Principles of Fair Information Practices

Fair information practices were originally identified by an advisory committee of the U.S. Department of Health, Education and Welfare in 1973 and form the basis for the Privacy Act of 1974, the legislation that protects personal information collected and maintained by the U.S. government. These principles were later adopted by the international community in the Organization for Economic Cooperation and Development's Guidelines for the Protection of Personal Data and Transborder Data Flows. Principles of fair information practices include consumer awareness, choice,

appropriate levels of security, and consumer access to their personally identifiable data. While the discussion that follows suggests ways in which these principles can be implemented, the private sector is encouraged to develop its own ways of accomplishing this goal.

1. *Awareness.* At a minimum, consumers need to know the identity of the collector of their personal information, the intended uses of the information, and the means by which they may limit its disclosure. Companies collecting and using data are responsible for raising consumer awareness and can do so through the following avenues:

- *Privacy policies.* Privacy policies articulate the manner in which a company collects, uses, and protects data, and the choices they offer consumers to exercise rights when their personal information is used. On the basis of this policy, consumers can determine whether and to what extent they wish to make information available to companies.
- *Notification.* A company's privacy policy should be made known to consumers. Notification should be written in language that is clear and easily understood, should be displayed prominently, and should be made available before consumers are asked to relinquish information to the company.
- *Consumer education.* Companies should teach consumers to ask for relevant knowledge about why information is being collected, what the

information will be used for, how it will be protected, the consequences of providing or withholding information, and any recourse they may have. Consumer education enables consumers to make informed decisions about how they allow their personal data to be used as they participate in the information economy. Consumer education may be carried out by individual companies, trade associations, or industry public-service campaigns.

2. *Choice.* Consumers should be given the opportunity to exercise choice with respect to whether and how their personal information is used, either by businesses with whom they have direct contact or by third parties. Consumers should be provided with simple, readily visible, available, and affordable mechanisms -- whether through technological means or otherwise -- to exercise this option. For certain kinds of information, e.g., medical information or information related to children, an affirmative choice by consumers may be appropriate. In these cases, companies should not use personal information unless its use is explicitly consented to by the individual or, in the case of children, his or her parent or guardian.