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

Attachment 2

Privacy Guidelines Commentary

Submitted with the Comments of the Online Privacy Alliance
On the Draft International Safe Harbor Principles

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.

2. Both the United States and Europe have long traditions of protecting individual privacy, and histories of debating on how best to protect individual liberties and private lives from intrusion. The European tradition follows the path of more reliance on government and complex codes and laws, many of which are to American eyes legally vague, overbroad, and be the potential source of significant legal exposure. The American tradition of protecting individual rights, including privacy, is to rely on the creation of private remedies, to engage the Members of the business community as citizens, to codify the developments of best practices in industry codes, and only in the event of concrete experienced harm, to legislate — and then to legislate with focused specificity. In this new electronic realm, where traditional jurisdictional borders cease to exist, the Alliance believes that the American practice may serve as an acceptable model for the development of privacy practices for businesses around the globe, and offer their efforts for emulation by business globally.

3. The "Membership" of the Alliance is drawn from a wide diversity of business sectors. Each sector has unique personal information requirements, management processes, and customer bases. 1/ Thus each Member has a set of unique opportunities to develop privacy practices and self-regulatory support and enforcement mechanisms that will respond most effectively to the concerns of the individuals with whom it deals. As a consequence of this diversity, the Guidelines often appear to speak in broad generalities; however, the intent of the Members was not to "generalize away" the protections that they intended to create or the privacy practices they are committed to instituting on-line. To the contrary, it is the occasional "generality" of certain of the provisions of the Guidelines that permits each company to fashion policies that protect privacy and empower consumers. This commentary is offered as a tool for assisting in the implementation of these efforts, so that results are consistent with the Guidelines' intent.

4. It also is acknowledged, and indeed even embraced, that the Guidelines are a work in process, and they reflect business responding to the perceived need for greater trust in the on-line and electronic commerce arena. Technological change is proceeding at such a pace that inflexible Guidelines would risk being obsolete before being put into practice. New technologies create new benefits for both business and consumers, and new risks. New technological tools may swiftly appear that must be taken into account in the development of different privacy practices. The challenge and the process are acknowledged in the Guidelines, and infuse their language.

1/ The Online Privacy Alliance is an ad hoc coalition of companies and associations. It has no official "members." For ease of reference, the companies and associations that have come together to form the Online Privacy Alliance are referred to as members, participants, or organizations throughout this commentary.

MISSION

5. The Mission statement sets the scope of work of the Alliance and focuses attention on the core of the Alliance' principles and the expected responses and general obligations of its Members. The purpose is to create an environment of trust and to foster the protection of individuals' privacy on-line and in electronic commerce. The discrete focus is on commerce on-line, and this Mission does not cover corporate intranets or any off-line transactions regarding personal information.

6. Critically, the Alliance supports self-regulation, built on existing law and regulation. This approach reflects the American tradition of business responding to the public's needs with a flexibility and speed that normal democratic governmental institutions cannot be expected to display. This comment is not intended as a criticism of these institutions, but an acknowledgment that the democratic process of law and regulation creation in the United States properly and necessarily is a time-consuming process. And the process often results in legislation establishing enforcement and regulatory devices that are static and cannot be synchronized with technology, business practices, and citizen expectations.

7. Electronic commerce is developing at such a rate that any legislative attempt at consumer privacy protection may be made irrelevant or confusing by new technology. The Mission statement therefore implicitly acknowledges the acceptance by its Members of the responsibility to create tools that will protect consumer privacy through the creation of new self-regulatory structures and principles, including enforcement mechanisms, and new empowerment technologies.

8. At the same time, the critical role of government is acknowledged in its call for Members to support compliance with and strong enforcement of applicable laws and regulations. Although not specifically referenced, this clause is intended to refer to the powers of the Federal Trade Commission (FTC) and those of the State Attorneys General under their respective consumer protection acts, to prosecute unfair or deceptive business practices and misleading advertising. A business that affirms it has a privacy policy or program and holds itself out to the public as operating in conformity therewith has assumed a serious commitment and is legally exposed if it does not honor the policy. In short, effective self-regulatory efforts rely heavily on the enforcement of existing law. The U.S. Congress has recognized the need for robust enforcement of law and last year increased the FTC's Consumer Protection enforcement funding by almost 40%.

9. No self-regulatory program involving protection of the public can work without public awareness of its existence and articulation of the expectations of the other interested parties in the process. The Mission statement specifically acknowledges this need. The Alliance will promote broad awareness of and participation in Alliance initiatives by businesses, nonprofits, policy makers and consumers; the next Mission statement reinforces this by calling for affirmatively seeking input into and support for its initiatives from all interested parties committed to privacy protection.

10. Finally, it should be noted that the Mission statement specifically identifies and comments on the need and obligation to protect our children. No other participants in the electronic commerce world are specifically referred to, and this reflects the concern the Alliance

Members have for children. It is expected that on-line businesses dealing with children and their personal information must take into account their unique situation and foster unique practices and policies to protect a group that is not old enough to protect itself.

THE PLEDGE

11. The Pledge needs no particular explanation — it is clear and concise. It calls for implementation by each Member of privacy policies, which are expected to be individualized to the Member's particular industry and business process, and place the Guidelines as the benchmark against which they will be measured. Whether to establish deadlines for such implementation was explicitly discussed. A consensus emerged that implementation must be accomplished by each Member as quickly as possible, within six months of joining the Alliance or by the close of 1998. The founding Members have their signatures on the Pledge, so to speak, and thus are now accountable to fulfill it.

12. Equally important, the Pledge commits the Member to participation in effective and "appropriate" self-regulatory enforcement activities and mechanisms. The term "appropriate" underscores again the fact that the Members may find different mechanisms to be appropriate to the delivery of recourse and redress to their divergent customer constituencies. But all will "participate," and this is understood to be not only the agreement of the Members to abide by the procedures and requirements of the self-regulatory mechanism they select, but also to participate in the creation and operation of that mechanism.

THE GUIDELINES

GENERAL OBSERVATION

13. The preamble to the Guidelines and the penultimate paragraph following Guideline 5 are important in setting forth an overall understanding of their scope. They underscore that these are minimum targets. The base target is reflected in that closing paragraph. They do not supersede obligations imposed on the Member by law, regulation, or legal process, such as a judicial judgment or a consent order. The Guidelines cover personally identifiable information in the on-line or electronic commerce environment, but not information that is proprietary, or from publicly available or public record information.

14. The exceptions for publicly available or public record information are inserted to ensure that a Member does not incur liability or responsibility for information whose accuracy depends on a third-party, frequently a government agency. A business is entitled to rely on the accuracy of that information as much as any other user of that information, and it should not be required to take responsibility for it in place of the public repository or other organization that provided it. The exception for proprietary information is made because of concern for the security of information that provides a competitive advantage to the company. This would not normally include information provided to a company by one of its customers, such as purchase history, credit card information, or names and addresses of gift recipients from the customer. Proprietary information would, in most cases, depending on the company's business, include demographic and psychographic overlays on the customer's files based on records from other

sources. These are considered proprietary, since their appearance and use would provide clues to the company's business strategy. Providing access to such information would not increase privacy protection.

15. Finally, it should be noted that the preamble says that the Guidelines should include "at least" the following elements, customized and enhanced as appropriate to the business or industry sector concerned. These Guidelines are not merely aspirational, they are minimums. This is reinforced by the reference in the last paragraph to the Organization for Economic Cooperation and Development ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

16. A comparison of the Guidelines to the OECD Guidelines is beyond this Commentary's scope, but the reference reflects that the OECD Guidelines were a major influence on their development, and that Members are urged to consider them in drawing their own policies. Explicitly, the Guidelines urge Members to study the internationally accepted OECD Guidelines in their privacy policy formulation and implementation. As a convenience, the OECD Guidelines are annexed to this Commentary.

GUIDELINE 1. ADOPTION AND IMPLEMENTATION OF A PRIVACY POLICY.

"An organization engaged in on-line 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 on-line privacy policies by the

organizations with which they interact; e.g., by sharing best practices with business partners."

17. This Guideline reflects the belief that privacy and the protection of personally identifiable information is not only an individual responsibility, nor simply a corporate responsibility, but a ***business community*** responsibility. It reminds the community that business is a seamless web of relationships within which information flows; it must be protected at each step. The Guideline looks inward toward the Member company, and outward to its business partners, to create that protective community. Thus the organization engaged in on-line activities or electronic commerce acknowledges that it **must adopt and implement** a policy to protect individually identifiable information. The term "individually identifiable information" is defined by reference to the World Wide Web Consortium's (W3C) definition of "Personally Identifiable Data" in its March 30, 1998 Vocabulary Specification (See http://www.w3.org/TR/1998/WD-P3P10-harmonization-19980330). This is one of the main legs of an organization's commitment under the Alliance Pledge. The organization is also urged to encourage similar action by its business partners.

18. The amount of corporate resource commitment inherent in the commitment to adopt and implement a privacy policy cannot be overstated. These are expensive and time-consuming exercises, often requiring significant corporate reengineering. This helps explain why the commitment to foster adoption of similar policies by business partners is not mandatory. Knowing the size of the task they themselves were facing, Alliance Members could not commit to do more than urge such adoption by their suppliers and vendors and corporate customers.

Subject to considerations arising under the antitrust laws, it would, of course, be entirely within the province of any company to declare as part of its privacy policy that it would only conduct business with partners who had such policies. This language does not exclude this possibility. Moreover, it would, of course, be expected that any Alliance Member who entrusts personally identifiable information to a third-party to perform a business operation on its behalf would ensure by contract for the continuity of its protection in that third-party's hands. The process of demanding contractual language expressing these concepts should expand the awareness of the principles inherent in these Guidelines, and thus encourage their adoption by other companies.

GUIDELINE 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."

19. The intention is that the Member's privacy policy be easy to find on its website, or other electronic commerce vehicle, such as the developing interactive technologies. A policy is no good unless it is made public in an understandable manner. And notice about what one will do with information provides little privacy protection if the notice is not given *at least* at the time the information is elicited. This Guideline combines in a practical and easy-to-read synopsis several elements of a number of OECD Guidelines, including the Openness Principle, the Collection Limitation Principle, and the Purpose and Use Limitation Principles. In many respects, given its level of detail, Guideline 2 has elucidated in a progressive manner some of the OECD Guidelines' more general principles, applying them to this new medium, without in any way disproving their continued viability.

20. Two points are worth noting in the first paragraph of Guideline 2. First, the Guideline does not specify size of type, or location on a website, or depth of detail or other fine points. Each Member shall have to make these decisions on its own within the common-sense rule: easy to find, read, and understand. Second, the on-line policy must be available to be *read before or simultaneously with any information collection or request.* Again, flexibility is retained to permit each Member to experiment with the placement and timing of notices of its policy, perhaps where information is to be typed in, perhaps with a warning window when information is "submitted" or gathered automatically. This language suggests that it is possible that data may be collected without conscious submission by the individual. This is permissible when and only

when notice of the policy is given either before or at the time data are captured. Although somewhat surprising, this is not inconsistent with the OECD Guidelines provided this is lawful and fair; the consent of the individual being required only "where appropriate." To the extent technology permits a Member to identify an individual without specifically requesting him or her to enter data, such as by automated identity determination, the Member will need to address how to provide the necessary notice simultaneously.

21. The second paragraph is explicit as to the contents of the policy, and includes presumably the elements that must be provided in a notice of the policy. These elements are intended to actualize the Purpose Specification Principle of the OECD Guidelines. In many, if not most, cases, it will be obvious what information is being collected, in others, it will not be so clear (such as click-stream data or navigational data), and a statement of the "not so obvious" will be necessary.

22. It is here that the fact the Guidelines set a minimum beyond which any Member is free to go in protecting privacy becomes most clear. For example, possible third-party distribution of information *must* be disclosed, and the available choices about the collection, use, and disclosure of the information *must* be given. Here, although mere mention of possible third-party distribution, without identifying those parties by name or even type of business, may be sufficient, most Members believe a clear articulation of intended third-party distribution is appropriate. Some Members strenuously agreed to allow for, in limited circumstances, mere disclosures of third-party distribution. As discussed below, in Guideline 3, this "limited circumstance" is intended solely for law enforcement, statutory, or other recognized third-party

transfers such as where a company shares data with credit-verification agencies. It must be remembered that disclosure of this lack of choice is required. (However, where a third-party's use of this information will be unrelated to the purpose for which it is collected, Guideline 3 advocates giving an opportunity to opt out of this disclosure.) Where a company may make diverse uses of its data, such as for marketing or research purposes, the policy must disclose what choices it gives the consumer in these matters. Nothing in this Guideline 2 restricts a Member from using the full range of choices in describing such recipients, or mandates a particular level of choice as to its collection, use, or distribution of the information. Thus companies are given a broad field of possibilities in responding to the privacy concerns of consumers, and consumers can provide their information or not, in accordance with their concerns.

23. The second paragraph of Guideline 2 further requires that the policy include a statement of commitment to data security, and the nature of that commitment receives substance in Guideline 4, Data Security. This clause must be read together with the next clause, which sets out what steps the company takes to ensure data quality and access. Here "data quality" must be read to mean the classical OECD formulation (most of which is restated in Guideline 5. Data Quality and Access), that is, its relevance to the purpose for which it is to be used, and its accuracy, completeness, and timeliness. (See OECD Data Quality Principle.) "Access" means the individual right to know whether a company maintains relevant individual information, and to have the relevant information communicated in a reasonable time, manner, intelligible form, and for a fee that is not excessive to ensure the data are accurate. Once again, provided the policy is

clear in its enunciation of these items, a company is free to explore a universe of possibilities, subject to the minimum standards set out in the following three Guidelines.

24. The last paragraph of this Guideline covers two distinct subjects. The first requires disclosure of the consequences of a refusal to provide information. In most cases, this will probably be obvious, as the company will not be able to provide a good or service without the required information, such as an address, or a valid credit card number or other verifiable payment mechanism. In other cases, this may be less clear, and will require significant thought and discussion, as when an on-line mortgage broker, for example, provides different levels of mortgage funding at different rates, depending on the clarity, or detail, of information provided.

25. The second sentence requires disclosure of the "accountability mechanism" that the Member uses and how one can contact the organization. This might have profited from being separated into its own paragraph, for it relates to one of the great OECD principles, which supports the entire privacy edifice, the Accountability Principle, and relates further to enforcement and redress. Again, however, alternative approaches are encouraged. The accountability mechanism can be anything from merely providing contact points with the customer service department of a company to active participation in a third-party verification program and display of a certifying "seal" on the website. This is discussed below under "Enforcement." Again, the universe of accountability mechanisms is expanding and diversifying rapidly, and no single mechanism may be appropriate to all sectors. Some mechanisms may not even have been developed yet. Some may require sophisticated fact-finding or technical knowledge; some may require immediate action and others may permit problems to be addressed

in a more leisurely fashion. The important point of the policy is that the Member disclose the choice he or she has made so an individual may have his or her concerns addressed.

GUIDELINE 3. CHOICE/CONSENT.

> **"Individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them on-line 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 on-line 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."**

26. This Guideline covers use of the collected information for a purpose unrelated to that for which it was gathered, either by the entity that originally gathered it, or by a third-party to whom it is distributed. Under Guideline 2, the intended use must be disclosed. The information may not be used by the gathering entity without extending to the individual "[a]t a minimum the opportunity to opt out of such [unrelated] use." Although the Guideline uses "should" language for opt out of third-party distribution, the vast majority of Members believe opt out is mandatory for all cases of unrelated use. The permissive "should" language was intended to

cover two situations: first where the third-party disclosure is pursuant to law, statute, regulation, or disclosed contract; and second, those business models where the service is provided in exchange for the provision of personal information, and the ability to use that information. Rather than attempt to cover the universe of "exceptions" in the Guidelines, the Members believe the standard should be interpreted as mandatory, with limited exceptions.

27. Whether a purpose is "unrelated" should be approached from a common-sense perspective. It should at a minimum be measured against the uses disclosed and the reasonable expectations of the individual. It is not acceptable to disclose that one will use the information for "any related business purpose now known or hereafter discovered by us" or the like. Some degree of specificity is required.

28. Opt-out is mandatory, "in the vast majority of cases," where a third-party to whom the information is distributed will use it for an *unrelated* purpose. It should be noted that this provision implies two things. First, a Member who outsources various of its functions in order to fulfill the "purpose for which the information is gathered" need not provide opt out. The provision of the information to the third-party is probably necessary for fulfillment of the Member's contracted obligation to the individual. Other "uses" of the information may be required for reasonable business purposes for successful completion of the company's undertaking to the consumer, such as using it to verify his or her creditworthiness or his or her address for the shipment of a product. Opt-out should not be necessary in this circumstance. Second, the opt out will normally apply to both the disclosure to the third-party and the unrelated use, unless this third-party is also performing a function of the information gatherer's

disclosed use and use can be limited. A third-party's merely storing data, or combining it with other data, thus would appear to be an unrelated use.

29. It is expected that an opt out must be given where unrelated use by a third-party is anticipated.

30. The last sentence of this Guideline reminds the reader that providing opt out for unrelated use is a minimum, for it suggests that "opt out" could also take the form of "consent" or "opt-in." The drafters wished to underscore that the exercise of choice in the on-line environment can be accomplished in numerous ways, and they encourage the use of new technological tools to empower consumers to exercise choice.

GUIDELINE 4. DATA SECURITY.

> **"Organizations creating, maintaining, using or disseminating individually identifiable information should take appropriate measures to ensure its reliability and should take reasonable precautions to protect it from loss, misuse or alteration. They should take reasonable steps to ensure 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."**

31. The coverage of this paragraph is broader than at first appears, for it applies not only to companies gathering information, but to those who maintain, use, or disseminate it, regardless of the source of the information. All companies in the information stream must take appropriate

measures to ensure its "reliability." The measures will vary with the sector and the type of information. Information used for medical treatment, or to make decisions of grave personal consequence to individuals, will conceivably require an enhanced set of measures. Reasonable precautions must be taken to protect against loss, misuse, or alteration. Again, "reasonableness" will be determined by the perceived gravity of consequences if the precautions fail, measured against the state of the art and best practices in preventing loss, misuse, or alteration.

32. "Security" in this context goes beyond prevention of unauthorized access, such as protection from hackers. It also means internal misuse of data by company personnel. The concept of "misuse" of data includes "unauthorized access," so that measures taken should include precautions against access by employees, contractors, and others who have no need for access to the data to fulfill their duties, or appropriate limitations on access to portions of files containing data irrelevant to their functions. Security protection may require thoughtful software and database structuring, appropriate periodic changes of passwords and access codes, meticulous attention to changes of personnel and levels of authorized access, and other recognized security precautions.

33. It should be noted that the security steps are designed to ensure "reliability," not "data quality." The "quality" of data refers to its accuracy, and its completeness and timeliness for the purpose for which it is to be used. "Reliability" refers to the non-altered state of the information as originally obtained and subsequently maintained.

34. Alliance Members are again obligated to take "reasonable" steps to increase an understanding of the Guidelines by undertaking to ensure that third parties who have access to this information adopt similar precautions. What steps are "reasonable" must again await practical experience, and take into account the kind and sensitivity of the information concerned. Members who handle financial or medical information that they share with business partners, or have processed by service providers, may find a greater need for detailed formal contracts to ensure a full appreciation of the necessary security precautions. Other businesses may be "reasonable" in relying on developing business practices. Nevertheless, the educational function of this requirement, and the intention to cascade "best practices," is clear.

GUIDELINE 5. DATA QUALITY AND ACCESS.

> **"Organizations creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to ensure 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 ensure 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."**

35. This section outlines data quality and access. Consumer access to database information serves three purposes. The first is assure that information used for substantive decision making is accurate and adequate for the purpose. US public policy has recognized the importance of access for this purpose, and it is covered by laws such as the Fair Credit Reporting Act.

The second purpose is knowledge; assuring consumers they have enough knowledge to participate in an information based economy and may exercise appropriate choice. Often access may be replaced by quality notice and consumer education materials in helping consumers understand the use of information. In fact, notices and education often do a better job of giving the consumer the context to make thoughtful choices.

Lastly, consumer access provides a check and balance. If collectors, storers, users and distributors of information are aware that the data they process will be visible to the consumer, they will be more thoughtful about the data they collect, how they use it, and who they share it with.

Much of the European concern about access rests on this third purpose. At the same time consumer access often requires system changes, consumer services, and security measures that are more expensive than the value they deliver. The open question is whether quality notices, combined with openness about commercial processes and products, and FTC Section 5 authority can create enough balance to act as a check.

Guideline 2 requires the company to inform individuals what steps it takes to ensure data quality. The data must be accurate, complete, and timely for the purposes for which they are to be used. The "purpose test" often involves the problem of whether or not harm can be caused to individuals because of lack of accuracy, completeness, or updating. Consequently, what is "reasonable" to ensure data quality may vary dramatically from business to business. Some businesses may need to verify certain information, or cross-check it. Under Guideline 2, these steps will need to be disclosed in the policy adopted by each Member, and significant variations in policies would not be unexpected.

36. The second paragraph represents the Alliance Members' best efforts to implement the OECD Individual Participation Principle and the guidance of the Department of Commerce in its "Elements of Effective Self-Regulation" (Annex II) in their businesses, and to provide "access" to **ensure data quality**. The Guidelines put data quality in a prime position, and "access" is one of the methods by which such quality can be ensured. It should be noted that access is not given for the sake of access, but to ensure the data is correct and up-to-date.

37. The requirement that Members have processes to correct inaccuracies would appear at first glance a mere restatement of a practical business principle. However, the Guideline now raises a practical business principle to the status of enforceable obligation. Members must have mechanisms in place that are carefully proscribed. They must be simple and easy to use, presumably by consumers, and that provide assurance that inaccuracies have been corrected. This latter phrase is intended to encourage Members to provide a "feedback mechanism" to consumers who request corrections to ensure that they are carried out, in lieu of an obligation to

provide a copy of all the information on file. In addition, the section suggests other practical means of ensuring data quality, which are self-evident.

38. Among the means of ensuring data quality are "reasonable and appropriate consumer access and correction." Because this is the only phrase in the Guidelines modified by both "reasonable" and "appropriate," it bears discussion in some depth. In American common law, the phrase "reasonable" generally indicates that a balance of cost versus benefit, of reference to expectations, of reference to technical art, must be made. Sometimes this is in the context of determining if an effort that it was alleged should have been made should in all similar circumstances be made, or whether a paradigmatic entity called a "reasonable man" would agree that an effort was, or was not, "reasonable." Not too dissimilarly, the word "appropriate" indicates a sense of being "fitted to," or "in good measure with" some other object. In short, whether an outlay of effort, or a failure to do so, is "reasonable" or "appropriate" is a conclusion, is contextual, and changes over time. Whether it was "reasonable" not to have a radar screen in a tugboat in New York Harbor depended on the state of the art of the development of radar, not whether other tugboats used radar. Thus the conclusion that in 1948 it was unreasonable not to have radar was made independently of whether it was "reasonable" in 1938. Consequently, these words are intended to permit the development and interpretation of this phrase regarding access to and correction of information by an individual to track the development of technology, consumers' expectations, and America's *mores* in this respect.

39. Finally, the word "access" should be clarified, and it is not perhaps an ideal term for what is intended, which is to provide a mechanism to ensure the consumer that the information

she has provided on-line is *accurate,* that the data has the *quality* anticipated. It is not intended to provide entrée into all information on the company's computer regarding the individual. Such "access" to information within a company's system would in many cases violate Guideline 4, Data Security, and might violate confidentiality commitments given to third-party information providers, or even the privacy of others. For example, a consumer's direct access to his or her customer file with a company might enable the commitment of serious fraud on the company, or even on the consumer, in the case of someone having stolen his or her identity. Only authorized personnel within the organization who are responsible for Data Quality should have true physical access to the computer database. What is intended is something very similar to that set out in the European Union's Data Protection Directive, which requires that a company provide an individual with a description of the kinds of personally identifiable information it has obtained on-line from the consumer, and determine if it can respond to the individual's concern or question with either partial or summary information. If the individual's concern is not satisfied, then the company may, if it is reasonable and appropriate in the circumstance, provide a copy of the information to the individual.

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.

46. Finally, the principles forbid sites from "enticing" 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. In essence, this protective principle restates for children the Purpose Specification Principle of the OECD Guidelines, but in even stricter terms. The Purpose Specification Principle requires disclosure of the purpose of the information collection and limits its use to that purpose or "not-incompatible" purposes. The Privacy Alliance Members have agreed that, in the case of children, the site's activity, which presumably attracts the child to the location, is itself the disclosure of intended use and purpose. Information collected is limited to only what is necessary and used only for that activity. There is no "not incompatible purpose" expansion of permissible use.

EFFECTIVE ENFORCEMENT OF SELF-REGULATION

47. The Alliance Guideline recommendation on self-regulation puts detail and substance into the OECD Accountability Principle. Effective enforcement of self-regulation requires:

(1) verification and monitoring; (2) complaint resolution; and (3) education and outreach, and is premised on compliance with an enforcement of existing law and regulation.

48. Given the unique and still developing nature of on-line commerce, where trust in how information is handled may not yet be well established, acceptable procedures should be created and administered by a third-party, whose presence can be simply and adequately demonstrated by the appearance of its seal of certification on the Member's website. The seal would indicate that the Member submits its privacy policies, and its compliance with its own policy, to third-party verification, and resolution of complaints by consumers through a credible dispute resolution mechanism.

49. The Alliance supports third-party enforcement programs that permit companies to display a seal that it is hoped will gain recognition by consumers as a symbol of assurance. The Alliance's analysis of an effective seal program, which bears some similarity to an independent auditor's verification of financial reporting, calls for verification and monitoring of compliance with the Member's policy, either through self-assessment or by a compliance review by the seal program operator. Whether this effort will be successful with consumers will in part depend on the public's understanding of the significance of a given seal, and its trust in the seal-giver's credibility.

50. Parallel to this seal-granting program, trust establishment demands a means for consumers to have complaints about the information-handling processes of Members resolved by

a process perceived to be independent and impartial. The work to date indicates that this process, and the institutions needed to provide it, are still in the process of formation.

51. The discussion of the Privacy Seal Programs advocated by the Alliance, including the characteristics of a program, the program's verification and monitoring obligations, the circumstances under which a seal might be revoked, and the structure of a consumer complaint mechanism are clear. The Alliance has outlined what a seal program provider must do in terms of scale, scope, and substance, to be considered to be providing an effective enforcement program. Thus the Alliance gives clear direction as to what a third-party validator of a Member's privacy program must do to provide an effective validation and enforcement service. This is a significant contribution to the literature on self-regulation. Whether one or more of such programs will prove successful, or even necessary, will no doubt be determined by market forces, but the exercise demonstrates that self-regulatory efforts by business can produce ingenious, unprecedented, and flexible consumer protection mechanisms.

ASSOCIATION POLICY

52. The Association Policy of the Alliance is self-explanatory, but merits the observation that it requires Association Members to encourage their Members to adopt privacy Guidelines consistent with the Alliance Guidelines. The Association Member itself agrees to adopt privacy Guidelines consistent with the Alliance Guidelines insofar as the Association engages in on-line activities. Although this commitment does not require the Association Member to adopt policies on behalf of its Membership that are similarly consistent, the Association does commit to

encourage its Members to do so. Again, the Guidelines look for a "cascade" and educational effect of their efforts in this regard.

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.

3. *Data Security*. Companies creating, maintaining, using or disseminating records of identifiable personal information should take reasonable measures to ensure its reliability for its intended use and should take reasonable precautions to protect it from loss, misuse, alteration, or destruction. Companies should also strive to ensure that the level of protection extended by third parties to whom they transfer personal information is at a level comparable to its own.

4. *Consumer Access.* Consumers should have the opportunity for reasonable,

appropriate access to information about them that a company holds, and be able to correct or amend that information when necessary. The extent of access may vary from industry to industry. Providing access to consumer information can be costly to companies, and thus decisions about the level of appropriate access should take into account the nature of the information collected, the number of locations in which it is stored, the nature of the enterprise, and the ways in which the information is to be used.

B. Enforcement.

To be effective, a self-regulatory privacy regime should include mechanisms to ensure compliance with the rules and appropriate recourse to an injured party when rules are not followed. Such mechanisms are essential tools to enable consumers to exercise their privacy rights, and should, therefore, be readily available and affordable to consumers. They may take several forms, as proposed below, and businesses may need to use more than one, depending on the nature of the enterprise and the kind of information the company collects and uses. The discussion of enforcement tools below is in no way intended to be limiting. The private sector may design the means to provide enforcement that best suits its needs and the needs of consumers.

1. *Consumer recourse.* Companies that collect and use personally identifiable information should offer consumers mechanisms by which their complaints can be resolved. Such mechanisms should be readily available and affordable.

2. *Verification.* Verification provides attestation that the assertions businesses make

about their privacy practices are true and that privacy practices have been implemented as represented. The nature and the extent of verification depends on the kind of information with which a company deals -- companies using highly sensitive information may be held to a higher standard of verification. Because verification may be costly for business, work needs to be done to arrive at appropriate, cost-effective ways to provide companies with the means to provide verification.

3. Consequences. For self-regulation to be effective, failure to comply with fair information practices should have consequences. Among these consequences may be cancellation of the right to use a certifying seal or logo, posting the name of the noncomplier on a publicly available "bad-actor" list, or disqualification from Membership in an industry trade association. Noncompliers could be required to pay the costs of determining their noncompliance. Ultimately, sanctions should be stiff enough to be meaningful and swift enough to ensure consumers that their concerns are addressed in a timely fashion. When companies make assertions that they are abiding by certain privacy practices and then fail to do so, they may be liable for fraud and subject to action by the FTC.

ANNEX II

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

(23rd September 1980)

THE COUNCIL,

Having regard to articles 1*(c), 3(a)* and *5(b)* of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

RECOGNISING:

- that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

  that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

  that transborder flows of personal data contribute to economic and social development;

  that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

Annex to the Recommendation of the Council of 23rd September 1980

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:

· *(a)* "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

(b) "personal data" means any information relating to an identified or identifiable individual (data subject);

(c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

- *(a)* the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

  (b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

  (c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

- *(a)* as few as possible, and

  (b) made known to the public.

5 . In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- *(a)* with the consent of the data subject; or

  (b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

- *(a)* to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

  (b) to have communicated to him, data relating to him

  - *within a reasonable time;*

  - *at a charge, if any, that is not excessive;*

- *in a reasonable manner; and*

- *in a form that is readily intelligible to him;*

- *(c)* to be given reasons if a request made under subparagraphs *(a)* and *(b)* is denied, and to be able to challenge such denial; and

(d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially

observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

- *(a)* adopt appropriate domestic legislation;

  (b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;

  (c) provide for reasonable means for individuals to exercise their rights;

  (d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and

(e) ensure that there is no unfair discrimination against data subjects.

PART FIVE. INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

- information exchange related to these Guidelines, and
- mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.