for the purpose for which it is provided and used.

## II. Principles for Users of Personal Information

A. Acquisition and Use Principles:
Users of personal information should recognize and respect the privacy interests that individuals have in the use of personal information. They should:

- 1. Assess the impact on privacy of current or planned activities in deciding whether to obtain or use personal information.
- 2. Obtain and keep only information that could be reasonably expected to support current or planned activities and use the information only for those or compatible uses.
  - B. Notice Principle:

Individuals need to be able to make an informed decision about providing personal information. Therefore, those who collect information directly from the individual should provide adequate, relevant information about:

- 1. Why they are collecting the information;
- 2. What the information is expected to be used for;
- 3. What steps will be taken to protect its confidentiality, integrity, and quality;
- 4. The consequences of providing or withholding information; and
  - 5. Any rights of redress.
  - C. Protection Principle:

Users of personal information should take reasonable steps to prevent the information they have from being disclosed or altered improperly. Such users should use appropriate managerial and technical controls to protect the confidentiality and integrity of personal information.

D. Fairness Principle:

Individuals provide personal information on the assumption that it will be used in accordance with the notice provided by collectors. Therefore, users of personal information should enable individuals to limit the use of their personal information if the intended use is incompatible with the notice provided by collectors.

E. Education Principle:

The full effect of the NII on the use of personal information is not readily apparent, and individuals may not recognize how their lives may be affected by networked information. Therefore, information users should educate themselves, their employees, and the public about how personal information is obtained, sent, stored, processed, and protected, and how these activities affect individuals and society.

## III. Principles for Individuals Who Provide Personal Information

A. Awareness Principle:

While information collectors have a responsibility to inform individuals why they want personal information, individuals also have a responsibility to understand the consequences of providing personal information to others. Therefore, individuals should obtain adequate, relevant information about:

- 1. Why the information is being collected;
- 2. What the information is expected to be used for;
- 3. What steps will be taken to protect its confidentiality, integrity, and quality;
- 4. The consequences of providing or withholding information; and
  - 5. Any rights of redress.
  - B. Redress Principles:

Individuals should be protected from harm caused by the improper disclosure or use of personal information. They should also be protected from harm caused by decisions based on personal information that is not accurate, timely, complete, or relevant for the purpose for which it is used. Therefore, individuals should, as appropriate:

- 1. Have the means to obtain their personal information and the opportunity to correct information that could harm them;
- 2. Have notice and a means of redress if harmed by an improper disclosure or use of personal information, or if harmed by a decision based on personal information that is not accurate, timely, complete, or relevant for the purpose for which it is used.

## **Commentary on the Principles**

## Preamble

- 1. The National Information
  Infrastructure ("NII"), with its promise of a seamless web of communications networks, computers, data bases, and consumer electronics, heralds the arrival of the information age. The ability to obtain, process, send, and store information at an acceptable cost has never been greater, and continuing advances in computer and telecommunications technologies will result in ever-increasing creation and use of information.
- 2. The NII promises enormous benefits. To name just a few, the NII holds forth the possibility of greater citizen participation in deliberative democracy, advances in medical treatment and research, and quick verification of critical information such as a gun purchaser's criminal record. These benefits, however, do not come without a cost: the loss of privacy.

Privacy in this context means "information privacy," an individual's claim to control the terms under which personal information—information identifiable to a individual—is obtained, disclosed and used.

3. Two converging trends—one social, the other technological—lead to an increased risk to privacy in the evolving NII. As a social trend, individuals will use the NII to communicate, order goods and services, and obtain information. But, unlike paying cash to buy a magazine, using the NII for such purposes will generate data documenting the transaction that can be easily stored, retrieved, analyzed, and reused. Indeed, NII transactional data may reveal who communicated with whom, when, and for how long; and who bought what, for what price. Significantly, this type of personal information—transactional data—is automatically generated, in electronic form, and is therefore especially cheap to store and process.

4. The technological trend is that the capabilities of hardware, software, and communications networks are continually increasing, allowing information to be used in ways that were previously impossible or economically impractical. For example, before the NII, in order to build a profile of an individual who had lived in various states, one would have to travel from state to state and search public records for information on the individual. This process would have required filling out forms, paying fees, and waiting in line for record searches at local, state, and federal agencies such as the departments of motor vehicles, deed record offices, electoral commissions, and county record offices. Although one could manually compile a personal profile in this manner, it would be a time-consuming and costly exercise, one that would not be undertaken unless the offsetting rewards were considerable. In sharp contrast, today, as more and more personal information appears on-line, such a profile can be built in a matter of minutes, at minimal cost.

5. In sum, these two converging trends guarantee that as the NII evolves, more personal information will be generated and more will be done with that information. Here lies the increased risk to privacy. This risk must be addressed not only to secure the value of privacy for individuals, but also to ensure that the NII will achieve its full potential. Unless this is done, individuals may choose not to participate in the NII for fear that the costs to their privacy will outweigh the benefits. The adoption of fair