

## OFFICE OF MANAGEMENT AND BUDGET

### National Information Infrastructure; Draft Principles for Providing and Using Personal Information and Commentary

**AGENCY:** Office of Management and Budget.

**ACTION:** Notice and request for comments.

**SUMMARY:** OMB is publishing these draft principles on behalf of the Privacy Working Group of the Information Policy Committee, Information Infrastructure Task Force. They were developed by the Working Group to update the Code of Fair Information Practices developed in the early 1970s.

**DATES:** Comments should be submitted no later than March 21, 1995.

**ADDRESSES:** Comments should be sent to the Working Group on Privacy c/o the NII Secretariat, National Telecommunications and Information Administration, U.S. Department of Commerce, Room 4892, Washington, D.C. 20230. The Principles and Commentary can be downloaded from the IITF gopher/bulletin Board System: 202-501-1920. The IITF gopher/bulletin board can be accessed through the Internet by pointing your gopher client to IITF.DOC.GOV or by telnet to IITF.DOC.GOV and logging in as GOPHER. Electronic comments may be sent to NII@NTIA.DOC.GOV

**FOR FURTHER INFORMATION CONTACT:** Mr. Jerry Gates, Chair, Privacy Working Group, Bureau of the Census, Room 2430, Building 3, Washington, D.C. 20233. Voice telephone: 301-457-2515. Facsimile: 301-457-2654. E-mail: GGATES@INFO.CENSUS.GOV

**SUPPLEMENTARY INFORMATION:** The following Principles and Commentary were developed by the Information Infrastructure Task Force's Working Group on Privacy with the goal of providing guidance to all participants in the National Information Infrastructure. (The Principles appear in plain text, and the Commentary appears in italics.) The Principles are intended to update and revise the Code of Fair Information Practices that was developed in the early 1970s. While many of the Code's principles are still valid, the Code was developed in an era when paper records were the norm.

The Working Group distributed a draft of the Principles and Commentary for comment in May 1994 via electronic mail and in a notice published in the **Federal Register**. Major resulting changes are: (1) The Commentary has

been incorporated into the Principles and has been modified to reflect changes to the principles, define terms, and to clarify areas of confusion; (2) the principles for Information Collectors have been incorporated into Principles for Users of Personal Information since some users also have a responsibility to inform and obtain consent for uses; (3) the Principles now require Information Collectors to conduct a privacy assessment before deciding to collect information; (4) the notice given to individuals becomes the determining factor for limiting the use of personal information; (5) the information an individual may access and correct is expanded; and (6) the provision of notice and a means of redress that was linked to "final actions" that may harm individuals is now based on an improper disclosure of information or the use of information that lacks sufficient quality.

Before issuing the Principles as a final product, the Working Group is proposing them for comment again. The Working Group recognizes that the Principles cannot apply uniformly to all sectors. They must be carefully adapted to specific circumstances, therefore, the Working Group asks that final comments focus on major concerns about applying the principles broadly. Sectorial concerns should be addressed as organizations develop internal principles.

Further, the Working Group debated the privacy rights of deceased persons and how they might be addressed in the Principles, but was not able to come to a conclusion. The Working Group also welcomes comments on whether and how the Principles should be revised to treat the rights of the deceased or their survivors.

**Sally Katzen,**

*Administrator, Office of Information and Regulatory Affairs.*

### Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information

#### Preamble

The United States is committed to building a National Information Infrastructure (NII) to meet the information needs of its citizens. This infrastructure, created by advances in technology, is expanding the level of interactivity, enhancing communication, and allowing easier access to services. As a result, many more users are discovering new, previously unimagined uses for personal information. In this environment, we are challenged to develop new principles to guide

participants in the NII in the fair use of personal information.

Traditional fair information practices, developed in the age of paper records, must be adapted to this new environment where information and communications are sent and received over networks on which users have very different capabilities, objectives and perspectives. Specifically, new principles must acknowledge that all members of our society (government, industry, and individual citizens), share responsibility for ensuring the fair treatment of individuals in the use of personal information, whether on paper or in electronic form. Moreover, the principles should recognize that the interactive nature of the NII will empower individuals to participate in protecting information about themselves. The new principles should also make it clear that this is an active responsibility requiring openness about the process, a commitment to fairness and accountability, and continued attention to security. Finally, principles must recognize the need to educate all participants about the new information infrastructure and how it will affect their lives.

These "Principles for Providing and Using Personal Information" recognize the changing roles of government and industry in information collection and use. Thus, they are intended to be equally applicable to public and private entities that collect and use personal information. However, these Principles are not intended to address all information uses and protection concerns for each segment of the economy or function of government. Rather, they should provide the framework from which specialized principles can be developed as needed.

### I. General Principles for All NII Participants

Participants in the NII rely upon the privacy, integrity, and quality of the personal information it contains. Therefore, all participants in the NII should use whatever means are appropriate to ensure that personal information in the NII meets these standards.

#### A. Information Privacy Principle:

An individual's reasonable expectation of privacy regarding access to and use of his or her personal information should be assured.

#### B. Information Integrity Principle:

Personal information should not be improperly altered or destroyed.

#### C. Information Quality Principle:

Personal information should be accurate, timely, complete, and relevant

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

information principles is a critical first step in addressing this concern.

6. While guidance to government agencies can be found in existing laws and regulations, and guidance to private organizations exists in principles and practices, these need to be adapted to accommodate the evolving information environment.\* This changing environment presents new concerns:

(a) No longer do governments alone obtain and use large amounts of personal information; the private sector now rivals the government in obtaining and using personal information. New principles would thus be incomplete unless they applied to both the governmental and private sectors.

(b) The NII promises true interactivity. Individuals will become active participants who, by using the NII, will create volumes of data containing the content of communications as well as transactional data.

(c) The transport vehicles for personal information—the networks—are vulnerable to abuse; thus, the security of the network itself is critical to the NII's future success.

(d) The rapidly evolving information environment makes it difficult to apply traditional ethical rules, even ones that are well understood and accepted when dealing with tangible records and documents. Consider, for example, how an individual who would never trespass onto someone's home might rationalize cracking into someone's computer as an intellectual exercise. In addition, today's information environment may present questions about the use of personal information that traditional rules do not even address.

7. These "Principles for Providing and Using Personal Information" (the "Principles") attempt to create a new set of principles responsive to this new information environment. The Principles attempt to provide meaningful guidance on this new information environment and attempt to strike a balance between abstract concepts and a detailed code. They are intended to guide all NII participants and should also be used by those who are drafting laws and regulations, creating industry codes of fair information practices, and designing private sector and government programs that use personal information.

8. The limitations inherent in any such principles must be recognized. As made clear in the Preamble, the

Principles do not have the force of law; they are not designed to produce specific answers to all possible questions; and they are not designed to single-handedly govern the various sectors that use personal information. The Principles should be interpreted and applied as a whole, and pragmatically and reasonably. Where an overly mechanical application of the Principles would be particularly unwarranted, phrases with the words "appropriate" or "reasonable" appear in the text. This flexibility built into the Principles to address hard or unexpected cases does not mean that the Principles need not be adhered to rigorously.

9. Moreover, the Principles are intended to be in accord with current international guidelines regarding the use of personal information and thus should support the ongoing development of the Global Information Infrastructure.

10. Finally, adherence to the Principles will cultivate the trust between individuals and information users so crucial to the successful evolution of the NII.

### **I. General Principles for All NII Participants**

Participants in the NII rely upon the privacy, integrity, and quality of the personal information it contains. Therefore, all participants in the NII should use whatever means are appropriate to ensure that personal information in the NII meets these standards.

11. Three fundamental principles should guide all NII participants. These three principles—information privacy, information integrity, and information quality—identify the fundamental requirements necessary for the proper use of personal information, and in turn the successful implementation of the NII

#### **I.A. Information Privacy Principle:**

An individual's reasonable expectation of privacy regarding access to and use of his or her personal information should be assured.

12. If the NII is to flourish, an individual's reasonable expectation of information privacy should be ensured. A reasonable expectation of information privacy is an expectation subjectively held by the individual and deemed objectively reasonable by society. Of course, not all subjectively held expectations will be honored as reasonable. For example, an individual who posts an unencrypted personal message on a bulletin board for public postings cannot reasonably expect that personal message to be read only by the addressee.

13. What counts as a reasonable expectation of privacy under the Principles is not intended to be limited to what counts as a reasonable expectation of privacy under the Fourth Amendment of the United States Constitution. Accordingly, judicial interpretations of what counts as a reasonable privacy expectation under the Fourth Amendment should not inhibit NII participants from applying the Principles in a manner more protective of privacy.

**I.B. Information Integrity Principle:**  
Personal information should not be improperly altered or destroyed.

14. NII participants should be able to rely on the integrity of the personal information it contains. Thus, personal information should be protected against unauthorized alteration or destruction.

**I.C. Information Quality Principle**  
Personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.

15. Finally, personal information should have sufficient quality to be relied upon. This means that personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.

### **II. Principles for Users of Personal Information**

**II.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.

16. The benefit of information lies in its use, but therein lies an often unconsidered cost: the threat to information privacy. A critical characteristic of privacy is that once it is lost, it can rarely be restored. Consider, for example, the extent to which the inappropriate release of sensitive medical information could ever be rectified by public apology.

17. Given this characteristic, privacy should not be addressed as a mere afterthought, after personal information has been obtained. Rather, information users should explicitly consider the impact on privacy in the very process of deciding whether to obtain or use personal information in the first place. In assessing this impact, information

\* For example, the Privacy Act of 1974, 5 U.S.C. 552a; or New York State Public Service Commission, Statement of Policy on Privacy and Telecommunication. March 22, 1991, as revised on September 20, 1991.

users should gauge not just the effect their activities may have on the individuals about whom personal information is obtained. They should also consider other factors, such as public opinion and market forces, that may provide guidance on the appropriateness of any given activity.

18. After assessing the impact on information privacy, an information user may conclude that it is appropriate to obtain and use personal information in pursuit of a current activity or a planned activity. A planned activity is one that is clearly contemplated by the information user, with the present intent to pursue such activity in the future. In such cases, the information user should obtain only that information reasonably expected to support those activities. Although information storage costs decrease continually, it is inappropriate to collect volumes of personal information simply because some of the information may, in the future, prove to be of some unanticipated value. Also, personal information that has served its purpose and can no longer be reasonably expected to support any current or planned activities should not be kept.

19. Finally, information users should use the personal information they have obtained only for current or planned activities or for compatible uses. A compatible use is a use of personal information that was within the individual's reasonable contemplation or sphere of consent when the information was collected. The scope of this consent depends principally on the notice provided by the information collector pursuant to the Notice Principle (II.B) and obtained by the individual pursuant to the Awareness Principle (III.A). Without this compatible use limitation, personal information may be used in ways that violate the understanding and consent under which the information was provided by the individual. This may subject the individual to unintended and undesired consequences, which will discourage further use of the NII.

#### II.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.

20. Personal information can be obtained in one of two ways: it can be either collected directly from the individual or acquired from some secondary source. By necessity, the principles governing these two different methods of obtaining personal information must differ. While notice obligations can be placed on all those who collect information directly from the individual, they cannot be imposed uniformly on entities that have no such direct relationship. If all recipients of personal information were required to notify every individual about whom they receive data, the exchange of personal information would become prohibitively burdensome, and many of the benefits of the NII would be lost. However, if such users intend to use the information for uses not compatible with the understanding and consent of the individual, individuals must be given the ability to limit such use (see II.D, the Fairness Principle). Accordingly, notice obligations apply only to those who collect personal information directly from the individual and any users who want to use the data for incompatible uses.

21. This requirement specifically applies to all parties who collect transactional data generated as a byproduct of an individual's participation in the NII. Such parties include not only the party principally transacting with the individual in order to provide some product or service but also to those transaction facilitators such as communication providers and electronic payment providers who help consummate these transactions. For example, if an individual purchases flowers with a credit card through an on-line shopping mall accessed via modem, the Notice Principle applies to all parties who collect transactional data related to the purchase; not only to the florist, but also to the telephone and credit card companies.

22. In sum, all parties who collect personal information directly from the individual—whether they are the party principally transacting with the individual or are merely a transaction facilitator—should provide a notice that will adequately inform the individual about what the information is expected to be used for, including current and planned activities, and expected disclosures to third parties.

23. By providing notice, information collectors afford the individual a meaningful opportunity to exercise judgment in accordance with the Awareness Principle (III.A). Together, the Notice Principle and the Awareness Principle highlight the interactive

nature of the NII and how responsibility must be shared between those who collect personal information and those who provide it. The importance of providing this notice cannot be overstated, however, since the terms of the notice determine the scope of the individual's consent, which must be respected by all subsequent users of that information.

24. Having said this, it is important to realize that what counts as adequate, relevant information to satisfy the Notice Principle depends on the circumstances surrounding the collection of information. In some cases, a particular use of personal information will be so clearly contemplated by the individual that providing formal notice is not necessary. For example, if an individual's name and address is collected by a pizza operator over the telephone simply to deliver the right pizza to the right person at the right address, no elaborate notice or disclaimer need precede taking the individual's order. However, should the pizza operator use the information in a manner not clearly contemplated by the individual—for example, to create and sell a list of consumers of pizzas containing fatty ingredients to health insurance companies—then some form of notice should be provided. In other cases, not every one of the components of the Notice Principle will need to be conveyed. For example, a long distance carrier that uses transactional data generated as part of a telecommunications transaction only to route calls and create accurate billings might need only provide notice of its data security practices.

25. While the Notice Principle indicates what might constitute the elements of adequate notice, it does not prescribe a particular form for that notice. Rather, the goal of the Principle is to ensure that the individual has sufficient information to make an informed decision. Thus the drafters of notices should be creative about informing in ways that will help the individual achieve this goal.

26. Finally, although the Notice Principle requires information collectors to inform individuals what steps will be taken to protect personal information, they are not required to provide overly technical descriptions of such security measures. Indeed, such descriptions might be unwelcome or unhelpful to the individual. Furthermore, they may be counterproductive since widespread disclosure of the technical security measures might expose system vulnerabilities, in conflict with the Protection Principle (II.C).

#### II.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.

27. On the NII, personal information is maintained in a networked environment, an environment that poses tremendous risk of unauthorized access, disclosure, alteration, and destruction. Both insiders and outsiders may gain access to information they have no right to see, or make hard-to-detect changes in data that will then be relied upon in making decisions that may have profound effects.

28. For example, our national health care system expects to become an intensive participant in the NII. Through the NII, a hospital in a remote locale will be able to send x-rays for review by a renowned radiologist at a teaching hospital in another part of the country. The benefits to the patient are obvious. Yet, such benefits will not be reaped if individuals refuse to send such sensitive data because they fear that the NII lacks safeguards needed to ensure that sensitive medical data will remain confidential and unaltered.

29. In deciding what controls are appropriate, information users should recognize that personal information should be protected in a manner commensurate with the harm that might occur if it were improperly disclosed or altered. Also, personal information collected directly from the individual should be protected in accordance with the information provided to the individual pursuant to the Notice Principle (II.B).

30. Finally, technical controls alone cannot provide adequate protection of personal information. Although technical safeguards are well-suited to protect against unauthorized outsiders, they are less well suited to protect against insiders who may be able to alter or delete data improperly without breaching any technical access controls. Therefore, to protect personal information, information users should adopt a multi-faceted approach that includes both managerial and technical solutions. One management technique, for example, could strive to create an organizational culture in which individuals learn about fair information practices and adopt these practices as the norm.

#### II.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.

31. Two principles work together to ensure the fair use of information in the NII. The Acquisition and Use Principle (III.A.2) requires information users to use personal information only for current or planned activities or for compatible uses. In conjunction with this principle, the Fairness Principle requires users to enable individuals to limit incompatible uses of personal information. Juxtaposed, these two principles highlight again the interactive and interrelated relationships on the NII, which require participants to share the power and responsibility for the proper use of personal information.

32. An incompatible use occurs when personal information is used in a way neither reasonably contemplated nor consented to by the individual when the information was collected. As explained earlier, the scope of this consent depends principally on the notice provided by the information collector pursuant to the Notice Principle (II.B) and obtained by the individual pursuant to the Awareness Principle (III.A).

33. An incompatible use is not necessarily a harmful use; in fact, it may be extremely beneficial to the individual and society. For example, society may benefit when researchers and statisticians use previously collected personal information to determine the cause of a potentially fatal disease such as cancer.

34. On the other hand, without some limitation, information use may know no boundaries. Without a Fairness Principle, personal information provided under the terms disclosed and obtained pursuant to the Notice (II.B) and Awareness (III.A) Principles may be used in ways that violate those terms and thus go beyond the individual's understanding and consent. To guard against this result, before information is used in an incompatible manner, such use should be communicated to the individual and his or her explicit or implicit consent obtained. The nature of the incompatible use will determine whether such consent should be explicit or implicit. In some cases, the consequences to an individual may be so significant that the prospective data user should proceed only after the individual has specifically opted into the use by explicitly agreeing. In other cases, a notice offering the individual the ability to opt out of the use within a certain specified time may be adequate. It is the responsibility of the

data user to ensure that the individual is able to prevent such incompatible use. Implicit in this principle is the idea that the original data collector will convey to every new user information about the original notice.

35. Having said this, it must be recognized that the Fairness Principle cannot be applied uniformly in every setting. There are some incompatible uses that will have no effect on the individual's information privacy interest. Research and Statistical studies may be an example. Obtaining the consent of the individual to participate in such studies will add cost and administrative complexity to the process without affecting the individual's information privacy interests. In other cases, the information is for a significant public need that would be thwarted by giving the individual a chance to limit its use, and society recognizes the need and authorizes the use in a highly formal, open way (typically in legislation). An example would be the collection of data to support a law enforcement investigation where obtaining a suspect's consent to a new use of what has become investigatory data would be unlikely and even asking for such consent could be potentially counterproductive to the investigation. Nevertheless, given the interactive possibilities that the NII offers, data users should be creative about finding ways to satisfy the Fairness Principle.

#### II.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.

36. The Education Principle represents a significant addition to the traditional Code of Fair Information Practices. There are many uses of the NII for which individuals cannot rely completely on governmental or other organizational controls to protect their privacy. Although individuals often rely on such legal and institutional controls to protect their privacy, many people will engage in activity outside of these controls, especially as they engage in the informal exchange of information on the NII. Thus, individuals must be aware of the hazards of providing personal information, and must make judgments about whether providing personal information is to their benefit.

37. Because it is important that information users appreciate how the NII affects information privacy, and that individuals understand the ways in which personal information can be used in this new environment, information users should participate in educating themselves and others about the handling and use of personal information in the evolving NII.

**III. Principles for Individuals Who Provide Personal Information**

38. As previously noted, the NII will be interactive. Individuals will not be mere objects that are acted upon by the NII; rather, they will actively participate in using and shaping the new information technologies and environments. In such an essentially interactive realm, individuals should assume some responsibility for their participation in instances where they can affect that participation. For example, where individuals will have choices about whether and to what degree personal information should be disclosed, they should take an active role in deciding whether to disclose personal information in the first place, and under what terms. Of course, in certain cases, individuals have no choice whether to disclose personal information. For example, if the individual wants to execute a transaction on the NII, personal information in the form of transactional data will necessarily be generated. Or, the choice may exist in theory only. For example, an individual may be permitted not to disclose certain personal information, although exercising such choice will result in the denial of a benefit that they cannot give up to participate fully in society—e.g., obtaining a license to drive an automobile. If individuals are to be held responsible for making these choices, they must be given enough information by information collectors and users to make intelligent choices.

**III.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.

39. The Awareness Principle, in conjunction specifically with the Notice Principle (II.B) and more broadly with the Education Principle (II.E), strives to cultivate an environment where individuals have been given the tools necessary to take responsibility over how personal information is disclosed and used.

40. Increasingly, individuals are being asked to surrender personal information about themselves. Sometimes the inquiry is straight-forward; for example, a bank may ask for personal information prior to processing a loan request. In such situations the purpose for which the information is sought is clear—to process the loan application. There may, however, be other uses that are not so obvious, such as using that information for a credit car solicitation.

41. Indeed, individuals regularly disclose personal information without being fully aware of the many ways in which that information may ultimately be used. For example, an individual who pays or medical services with a credit card may not recognize that he or she is creating transactional data that could reveal the individual's state of health. The Awareness Principle encourages individuals to learn about and take into consideration such consequences before participating in these kinds of transactions.

**III.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.

42. There will be times when individuals are harmed by the improper disclosure or use of personal information. Individuals will also be harmed by the use of personal information that lacks sufficient quality to ensure fairness in that use. It is therefore important to implement measures to avoid or limit that harm, as well as measures to provide relief should harm occur.

43. Therefore, individuals should be able to obtain from information users, as appropriate, a copy of their personal information and have the opportunity to correct information about them that lacks sufficient quality to assure fairness in use and thus prevent potential harm. Whether this opportunity should be granted depends on the seriousness of the consequences to the individual of the use of the information. Finally, appropriate forms of redress should be available for individuals who have been harmed by the improper disclosure or use of personal information, or by the use of personal information that lacks sufficient quality to be used fairly. The Principles envision various forms of redress including, but not limited to, mediation, arbitration, civil litigation, regulatory enforcement, and criminal prosecution, in various private, local, state, and federal forums with a goal of providing relief in the most cost-effective, efficient manner possible.

**Appendix I. Principles for Providing and Using Information in the NII—Comparison of May 25, 1994, and Revised Version**

*I. General Principles for the National Information Infrastructure*

Participants in the NII rely upon the privacy, integrity, and quality of the personal information it contains. Therefore, all participants in the NII should use whatever means are appropriate to ensure that personal information in the NII meets these standards.

Original Version—May 25, 1994	Revised Version	Change
<p><b>A. Information Privacy Principle</b> Individuals are entitled to a reasonable expectation of information privacy.</p>	<p>An individual's reasonable expectation of privacy regarding access to and use of his or her personal information should be assured.</p>	<p>Moves principal from abstract "expectation," to an assurance that is the responsibility of all participants.</p>

Original Version—May 25, 1994	Revised Version	Change
<p><b>B. Information Integrity Principles</b></p> <p>Participants in the NII rely upon the integrity of the information it contains. It is therefore the responsibility of all participants to ensure that integrity. In particular, participants in the NII should, to the extent reasonable:</p> <ol style="list-style-type: none"> <li>1. Ensure that information is secure, using whatever means are appropriate;</li> <li>2. Ensure that information is accurate, timely, complete, and relevant for the purpose for which it is given.</li> </ol>	<p>Personal information should not be improperly altered or destroyed.</p>	<p>Principle has been revised to focus on traditional security definition of data integrity—guarding against improper alteration or destruction. Data quality attributes provisions have been moved to new principle: Information Quality Principle, below.</p>
<p><b>C. Information Quality Principle (NEW)</b></p> <p>(Partly contained in Information Integrity Principle.).</p>	<p>Personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.</p>	<p>New principle, but broken out of old Integrity.</p>

OLD II. Principle for Information Collectors (i.e. entities that collect personal information directly from the individual)—This principle has been deleted and its provisions moved to the Information Users Principles as the new “Notice Principle.”

Original Version—May 25, 1994	Revised Version	Change
<p><b>A. Collection Principle</b></p> <p>Before individuals make a decision to provide personal information, they need to know how it is intended to be used, how it will be protected, and what will happen if they provide or withhold the information. Therefore, collectors of this information should tell the individual why they are collecting the information, what they expect it will be used for, what steps they will take to protect its confidentiality and integrity, the consequences of providing or withholding information, and any rights of redress.</p>	<p>NA .....</p>	<p>Principle moved to and combined with the Principles for Information Users.</p>

New II. Principles for Information Users (i.e. Information Collectors and entities that obtain, process, send or store personal information).

Original Version—May 25, 1994	Revised Version	Change
<p><b>A. Acquisition and Use Principles</b></p> <p>Users of personal information must recognize and respect the stake individuals have in the use of personal information. Therefore, users of personal information should:</p> <ol style="list-style-type: none"> <li>1. Assess the impact on personal privacy of current or planned activities before obtaining or using personal information.</li> <li>2. Obtain and keep only information that could reasonably be expected to support current or planned activities and use the information only for those or compatible purposes.</li> <li>3. Assure that personal information is as accurate, timely, complete and relevant as necessary for the intended use..</li> </ol>	<p>Users of personal information should recognize and respect the privacy interests that individuals have in the use of personal information. They should:</p> <ol style="list-style-type: none"> <li>1. Assess the impact on privacy of current or planned activities in deciding whether to obtain or use personal information.</li> <li>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.</li> </ol>	<p>The assessment in paragraph 1, now precedes a decision to collect data, not merely the data collection itself.</p> <p>The original paragraph 3, placing responsibilities on users to assure data quality has been moved to the Information Quality Principle in Section I to emphasize that this is a responsibility of all parties.</p>

**B. Notice Principle** (This is a new principle for this section. It recognizes that notice is a critical element in the successful establishment of the Principles as a working set of guidelines. Adequate notice will ensure that information acquisition and usage occurs within the knowledge and consent of the individual who provides it. Because users may wish to use information for purposes that are incompatible with that knowledge and consent, the principle states that before such use can occur, the individual must be renotified and his or her consent obtained.)

Original Version—May 25, 1994	Revised Version	Change
(Originally contained in the "Collector 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: <ol style="list-style-type: none"> <li>1. Why they are collecting the information;</li> <li>2. What the information is expected to be used for;</li> <li>3. What steps will be taken to protect its confidentiality, integrity, and quality;</li> <li>4. The consequences of providing or withholding information; and</li> <li>5. Any rights to redress.</li> </ol>	Moved from "Collector Principle" to emphasize responsibility of both collectors and certain users to inform individuals of the uses of their data and to obtain their knowledge and consent to such uses.

### C. Protection Principle (renumbered as C.)

Original Version—May 25, 1994	Revised Version	Change
Users of personal information must 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.	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.	Changes verb "must" to "should" for consistency with other wording throughout the Principles.

**D. Fairness Principles** (This Principle has been moved up to emphasize the importance of users treating information providers fairly.)

Original Version—May 25, 1994	Revised Version	Change
Because information is used to make decisions that affect individuals, those decisions should be fair. Information users should, as appropriate: <ol style="list-style-type: none"> <li>1. Provide individuals a reasonable means to obtain, review, and correct their own information.</li> <li>2. Inform individuals about any final actions taken against them and provide individuals with means to redress harm resulting from improper use of personal information;</li> <li>3. Allow individuals to limit the use of their personal information if the intended use is incompatible with the original purposes for which it was collected, unless that use is authorized by law.</li> </ol>	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.	The Principle has been simplified. It looks to the notice given under the Notice Principle as the determinant of when individuals should be given the ability to limit use of their personal information. The redress provisions of the original formulation have been incorporated into the Notice Principle above and to the Redress Principles in Section III. The Commentary provides guidance on what constitutes a "compatible" and "incompatible" use.
<p><b>E. Education Principle</b></p> <p>The full effect of the NII on both data use and personal privacy is not readily apparent, and individuals may not recognize how their lives can be affected by networked information. Therefore, information users should educate themselves, their employees, and the public about how personal information is obtained, sent, stored and protected, and how these activities affect others.</p>	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.	Expands education principles to include societal effects given the potential effect of the NII on social structures and relationships.

Original Version—May 25, 1994	Revised Version	Change
<p><b>III. Principles for Individuals who Provide Personal Information</b></p> <p><b>A. Awareness Principles</b></p> <p>While information collectors have a responsibility to tell individuals why they want information about them, individuals also have a responsibility to understand the consequences of providing personal information to others. Therefore, individuals should obtain adequate, relevant information about.</p> <ol style="list-style-type: none"> <li>1. Planned primary and secondary uses of the information.</li> <li>2. Any efforts that will be made to protect the confidentiality and integrity of the information.</li> <li>3. Consequences for the individual of providing or withholding information.</li> <li>4. Any rights of redress the individual has if harmed by improper use of the information.</li> </ol> <p><b>B. Redress Principles</b></p> <p>Individuals should be protected from harm resulting from inaccurate or improperly used personal information. Therefore, individuals should, as appropriate.</p> <ol style="list-style-type: none"> <li>1. Be given means to obtain their information and be provided opportunity to correct inaccurate information that could harm them.</li> <li>2. Be informed of any final actions taken against them and what information was used as a basis for the decision.</li> <li>3. Have a means of redress if harmed by an improper use of their personal information.</li> </ol>	<p>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:</p> <p>.....</p> <ol style="list-style-type: none"> <li>1. Why the information is being collected;</li> <li>2. What the information is expected to be used for;</li> <li>3. What steps will be taken to protect its confidentiality, integrity, and quality;</li> <li>4. The consequences of providing or withholding information; and.</li> <li>5. Any rights of redress.</li> </ol> <p>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:</p> <ol style="list-style-type: none"> <li>1. Have the means to obtain their personal information and the opportunity to correct information that could harm them.</li> <li>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.</li> </ol>	<p>Description of what information individual should obtain to make informed decision to provide data has been simplified.</p> <p>Redress section has been rewritten to expand the scope of its provisions. Whereas original formulation restricted individuals ability to correct information that could harm them to only "inaccurate" information, revised draft includes any of the information quality attributes from the Information Quality Principle as a basis: e.g., incomplete information.</p> <p>Original paragraphs 2 and 3, stating that individuals should be informed of "final actions" taken against them and have a means of redress if harmed by improper uses of their personal information has been consolidated into one new paragraph. The "informed of any final actions" thought has been discarded because of the difficulty of arriving at an adequate definition of what constitutes a "final action." Instead, it has been replaced with a provision for "notice and means of redress" for improper disclosures of information, or for use of data that lacks sufficient quality as explained by the Information Quality Principles.</p>

[FR Doc. 95-1480 Filed 1-19-95; 8:45 am]

BILLING CODE 3110-01-P-M