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

<sup>\*</sup> 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.