# USA'S PRIVACY PRINCIPLES FOR NATIONAL INFORMATION INFRASTRUCTURE

***The United States is building a National Information Infrastructure (NII) to meet the information needs of its citizens. As part of this process, the Information Infrastructure Task Force's Working Group on Privacy issued draft principles and a commentary on 21st April 1994 to guide NII users. The aim of the principles is to ensure fair use of personal information. It is intended that they will update the Code of Fair Information Practices developed in the early 1970's. The Working Group invited public comments on the principles and commentary and is currently revising the draft. Stewart Dresner, Privacy Laws & Business Director, gave his comments in May in Washington to Robert Veeder, the chairman of the Working Group on Privacy.***

The National Information Infrastructure (NII) came into being as a result of the rapid advances in computer and communications technology. It is expanding the scope of interactivity and communications which provide access to services and users. The NII is a web of communication networks, computers, databases, and consumer electronics where vast amounts of information (including sensitive information) will be available on-line and can be accessed by a large number of users.

The *Principles for Providing and Using Personal Information* are intended to be applicable to those who collect and use personal data, in both public and private sectors. They acknowledge that all members of society should share responsibility for ensuring fair treatment of individuals in the use of their personal information. However, the principles are not intended to address all information uses for each specific segment of the economy or government but to provide a wide framework from which specialised principles can be developed sector by sector. They are defined in broad terms and only address information identifiable to a living individual.

## 1. General Principles for the National Information Infrastructure

The general principles apply to all NII participants: information collectors, users and individuals, and relate to privacy and information integrity.

**A. Information Privacy Principle**

Individuals are entitled to a reasonable expectation of information privacy.

**B. Information Integrity Principles**

NII users should, to a reasonable extent, ensure that:

- information is secure, using whatever means are appropriate
- information is accurate, timely, complete and relevant for the purpose for which it is given.

## 2. Principle for Information Collectors

This principle applies to organisations that collect personal information directly from the individual.

**Collection Principle**

Collectors of information should inform the individual of the reason for collecting the information, what they expect it will be used for, what steps will be taken to protect its confidentiality and integrity, the consequences of providing or withholding information and any rights of redress.

## 3. Principles for Information Users

The following four principles are intended to include both information collectors who have direct links with the individuals, and collect information from them directly, and those organisation which do not. They were drafted in this manner as it was considered difficult to impose the information collector obligations on organisations with no direct links with the individuals.

**A. Acquisition and Use Principles**

Users of personal information should:

- assess the impact on personal privacy of current or planned activities before obtaining or using the information,

- 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,
- ensure that personal information is accurate, timely, complete and relevant as necessary for its intended use.

**B. Protection Principle**

Users of personal information must take the necessary steps to prevent unauthorised disclosure and alteration. To this end they should use appropriate managerial and technical controls to protect the confidentiality and integrity of personal information.

**C. Education Principle**

Information users should educate themselves, their employees and the public about how personal information is obtained, transmitted, stored and protected.

**D. Fairness Principle**

Information users should:

- provide individuals with reasonable means to obtain, review, and correct their own information,
- provide individuals with the means to redress harm resulting from improper use of personal information,
- allow individuals to limit the use of their personal information if the intended use is incompatible with the original purpose for which it was collected, unless the use is authorised by law.

## 4. Principles for Individuals who Provide Personal Information

Individuals must take an active role in deciding whether to disclose their information in the first instance. In order to do that, they should receive meaningful information on the intended uses of the information they provide, and they have a responsibility to understand the consequences of providing or withholding personal information. These principles may be expressed in two categories which apply to individuals: awareness and redress.

**A. Awareness Principle**

Individuals should obtain adequate and relevant information about:

- the planned primary and secondary uses of the information,
- the measures that will be taken to protect the confidentiality and integrity of their information,
- the consequences of providing or withholding personal information,
- the rights of redress if they are harmed by improper use of the information.

**B. Redress Principle**

Individuals should, as appropriate:

- be given the means to obtain their information and have the opportunity to correct inaccurate information that could harm them;
- be informed of any action taken against them and what information was used as a basis for the decision;
- have a means of redress if harmed by improper use of their personal information.

The draft *Principles for Providing and Using Personal Information and Commentary* are available from the Working Group on Privacy c/o the NII Secretariat, National Telecommunications and Information Administration, US Department of Commerce, Washington DC, 20230, USA. Electronic comments should be sent to the Information Infrastructure Task Force Bulletin Board System (IITF BBS) + (1) 202 501 1920. The IITF BBS can be accessed through the Internet by pointing your Gopher Client to iitf.doc.gov and login as gopher.

A critique of the above principles has been prepared by David Banisar, a policy analyst, at the Electronhic Privacy Information Centre (EPIC), 666, Pennsylvania Aveneue, SE Suite 301, Washington DC 20003, USA.
Telephone: + (1) 202 544 9240
Fax: + (1) 202 547 5482
Electronic mail: (Banisar @epic.org)

**This report was written by Dr. Deborah Fisch Nigri, *a Privacy Laws & Business* consultant.**