2.3. Other Codes and Comments

J. Berleur et al. (eds.), *Ethics of Computing*

Standards of Computer Science Deontology of CITEMA

Centro de la Informática, Telemática y Medios Afines (Spain)

1. *In the exercise of their professional activities, informaticians*[1] *will strive to spread the knowledge of computer science principles, the tools used in the information process, and the precise value of the results. They will oppose all false, inexact or exaggerated claims about computer science.*

The diffusion of scientific and professional techniques is constant in all deontological codes from the "Hippocratic Oath" to the latest texts.

In the computer science profession, this moral duty is of special importance. The rapid development of computer science techniques has given rise to a lot of mistaken concepts, even myths, about computers. For example, calling computers "electronic brains" (with all the ambiguous consequences that expression can bring) is symptomatic of a latent belief in the so-called, magical ("miracle-working") qualities of computers. That is why the obligation to oppose false, inexact or exaggerated claims has been associated with the obligation to teach about computer science.

2. *Informaticians will only accept professional jobs which they are able to do, and whose completion can be supported by technical or scientific knowledge. In the opposite case, they must advise the client of the limitations of the computer science systems, as well as any danger of errors and biases that may lead to improper manipulation of data results.*

The dangers of misuse of computer science, as well as the possibilities for its irresponsible use, must always be made clear. In the legal field, it would not be easy to insist on penal or civil responsibility for any harm that such use might cause. That would involve the expression of a moral criterion which would force professionals to warn their client or employer of the inherent dangers.

Some examples of cases where users must be warned of the dangers and risks of data processing include electoral polls, market research and other similar applications.

3. *Informaticians will contribute to the progress of computer science and information processing, exchanging documentation and expertise with other professionals and specialists. They will not hide any knowledge and experience acquired which could aid the development of computer science.*

This rule calls our attention to the moral inadmissibility of monopolizing particular techniques or information with a view to exploiting this advantage (for example, rapid technological access to the most advanced techniques that other professionals perhaps do not have). Abuse of this situation of privilege would be morally illicit.

4. *Informaticians will never take personal advantage or benefit of access to files and equipment of which they are in charge in the course of their jobs.*

This standard does not require further explanation. In pure deontology it is illicit to create indefensible situations.

5. *Informaticians will always bear in mind the demand for the protection of information. They will avoid any levity or negligence*

[1] Europeans tend to refer to information technology as informatics, and personnel working in the informatics field as informaticians.

which could alter or destroy data held on processing equipment.

Protecting the physical integrity of data requires careful use of measures, means and techniques to prevent the information from being altered or erased, with all the disadvantages of any error or accident which could occur.

6. *Informaticians will refrain from copying any data (with or without any intention to profit) without a responsible person's authorization.*

They will never appropriate programs of which they may have knowledge in the exercise of their jobs, nor routines, nor other parts of the same, nor the equipment on which they are held.

Both these rules must not be understood as intending to protect a God-given right or of any other nature to data or programs. Rather, they are associated with the fourth standard (above). They are deontological rules linked to legal rules about the illicit nature of indefensible situations.

7. *Due to their professional activities, if informaticians have access to information transmitted between time-sharing systems, they will maintain that information with absolute secrecy.*

This deontological rule is conceived to deal with the problems of conscience that can arise in a specific computer science situation, one that is likely to be more common in the near future and that will be diversified according to the practical circumstances.

8. *Informaticians will not transfer or disclose to any third party the personal or intimate data held in databases to which they have access in the exercise of their jobs.*

By personal and intimate data, we especially understand data that refer to one or more of the following: employment relations, fiscal duties, insurance, criminal history, namely related to political, ideological or religious activities, marital status, commercial solvency, banking or saving accounts, educational history, properties, etc. (This list is not comprehensive.) The concept of the private sphere is that of personal information or data whose distribution is to be considered a personal decision made by the persons involved. The data is not necessarily personal information of an intimate character, but it is information which we normally assume that a particular individual (not a public person, like an artist, politician, etc.) wishes to protect.

9. *Informaticians will only provide personal data when they are bound to do so for legal reasons of common good* [2] *or public interest.*

This rule is the logical counterbalance to the previous rules. If moral prohibitions about improper use or acquisition of personal information are followed to their end, they can lead to results opposed to the very purposes initially intended. Conflicts can arise between the duty to respect privacy and the demands of common good . At a deontological level, the prime importance of common good is clear, as we determined earlier[3]. Though the point of reference in this ninth rule is legal measures which are mandatory for conscience, from the moral and deontological aspect, it is necessary to submit the adequacy of these measures to the "fireproofing" of common good or public interest.

10. *The persons who represent the Administration as well as the titular or the executive body to which the exercise of discretionary power falls in relation to computer science will always respect the personality of the persons being administered and their privacy.*

This is a general deontological principle which refers to Administration. Because Administration is essentially impersonal, here the deontological norms are addressed to the physical persons who adopt decisions legally binding on their members on behalf of the Administration.

This general standard can be developed into more concrete rules. A wide variety of

---

[2] The Spanish text uses "Bien Común", "Common Good". We could have used here "public welfare" *(Note of the Editor).*

[3] The Preamble to which it is referred here, as well as the Preliminary Note mentioned in Standard 10, have not been provided. *Note of the Editor.*

criteria, ranging from the deontological orientation of the civil servant to the promulgation of laws or specific regulations, exist in all countries and have led to the creation of institutional measures of control. The purpose which serves as a basis in writing these rules, as given in the Preliminary Note, prevents great precision in developing the given general rule. On the contrary, it could act as a guide in areas foreign to that purpose as, for example, when elaborating authentic and proper legal rules or in establishing professional corporations.

CITEMA, Plaza Alonso Martínez 3, 2° Dcha., 28004 MADRID, SPAIN (Phone: +34 1 448-4795; Fax: +34 1 448-2871)

English translation provided by Porfirio BARROSO, February 1994, revised by Diane WHITEHOUSE and the Editor.

Comments on Standards of Computer Science Deontology of CITEMA

Porfirio BARROSO and María Angeles NEVADO
University of Madrid

PROFILE AND CONSTITUTION OF CITEMA

The Guidelines of Computer Science Deontology of CITEMA were written by Dr. José Carlos-Roca Rovira, Dr. Manuel Heredero Higueras, Dr. Luis Navarro Gil and Mr. Ramón Villanueva Etcheverría in 1974.

CITEMA is a Cultural Foundation approved by the Spanish Ministry of Education on April 8th, 1969.

CITEMA is a member of FESI (Federación Española de Sociedades de Informática: Spanish Federation of Computer Science Societies) a not-for-profit organization. It is composed of highly qualified experts in computer science.

MEMBERSHIP STRUCTURE

Members consist of two kinds:

2.1. Collective members: Institutions, Firms, Organizations.

2.2. Individual Members.

Any person or institution can join CITEMA by voluntary decision. Members commit to paying the fees for the society's upkeep.

RULES OF ENFORCEMENT

CITEMA rules were put into effect in 1974, and they are still working today.

These rules oblige each member of CITEMA to fulfil his/her commitments as a member.

PROCESS OF UPDATING AND ENHANCEMENT OF THE CODE

CITEMA rules were put into effect in 1974, and have not been revised since.

EDUCATION OF THE MEMBERS IN THE ETHICAL FIELD OR THROUGH EDUCATIONAL INSTITUTIONS

The CITEMA organization does not discuss the education of its members in the ethical field.

PUBLICATION SERVICE

CITEMA publishes a 120-page bulletin twice a year.

This journal reports news about information and data processing (methodology and organization), and so on.

The bulletin publishes annexes which include indexes from computer science journals, and some articles which report on computer ethics.

The most important objective of CITEMA is the organization of the SIMO (Semana Internacional del Mueble de Oficina), an Annual International Exhibition covering all kinds of computer science supplies.

CITEMA (SIMO) distributes an Annual Catalogue (1,000 pages in length) of office supplies and computer science material, with a list of registered trademarks in up-to-date markets.

TRAINING OR RE-TRAINING SERVICE

CITEMA organizes Congresses, Conferences, Seminars, Workshops, Round Table Conferences, and Meetings about computer ethics.

RESEARCH SERVICE

One of the purposes of CITEMA is to report on marketing by manufacturers and vendors of computer science materials and office supplies.

EXHIBITION SERVICE

CITEMA organizes an International Trade Fair of office supplies and computer science mate-

rials (SIMO), and it also exhibits books published on these subjects.

INFORMATION SERVICE

CITEMA answers any question or request in writing about any theme in its area of specialization.

ITEMS WHICH ARE NOT INCLUDED IN THE CODE OF CITEMA

We comment briefly on the Standards of Computer Science Deontology of CITEMA. The code is composed of ten issues or standards on computer ethics.

We only mention the rules which are not included in the code[4]. These rules are:

1. Professional responsibility of the informatician at work.
2. Loyalty or faithfulness of the informatician to his/her firm, country and the public.
3. Dignity, honesty, integrity of the computer expert.
4. Professional solidarity of the informatician.
5. The computer expert should transmit data with accuracy.
6. Professional ability of the informatician.
7. The informatician should avoid conflicts of interest.
8. Fair competition among computer technicians.
9. The computer expert has the moral obligation to fulfill deontological rules.
10. The informatician must respect the professional code of ethics.
11. Discretion and prudence of the computer technician in his/her tasks.
12. The computer expert must respect Constitutions and Laws.
13. The informatician must not discriminate against any person because of race, religion, colour, sex, ideology or nationality.
14. The computer technician should not mix private life with professional life.
15. The informatician must work full-time for the profession.
16. The computer technician must respect the public's Right to Reply, and correct his or her mistakes.

---

[4] See Jesus Maria VAZQUEZ and Porfirio BARROSO, *Deontologia de la Informatica. Esquemas*, Madrid, Instituto de Sociologia Aplicada, 1993.

Health Informaticians' Deontology Code (HIDEC) - Greece

PROLEGOMENA

The here presented Health Informaticians' Deontology Code (HIDEC) has to be considered as a 'filtrate' of present research.[1] In the future, possible application of HIDEC will lead to include Greek particularities which cannot be defined *a priori*. For clarifying the Greek situation, the reader could refer to Gritzalis et al. (1991)[2] and to 'The Greek Data Protection Bill' (1988)[3]. It should be noted that in Greece there is no legislation on data protection in the health area. The health data are vaguely protected by medical ethics.

The HIDEC cannot be static. The evolution of informatics and social systems will be affecting it proportionally. So, there will be a need for continuous revision. An important remark is that access to the health informatician (h.i.) cannot be excluded from health data which refer to the doctor and his patient[4].

INDIVIDUAL PROFESSIONAL DEONTOLOGY

Social responsibility

The h.i. uses his specialization for the promotion of health and quality of life. He has a moral obligation to assess the social impacts of his activities and to contribute to the safe and beneficial use of the applications of informatics.

Protection of the Individuality

The h.i. respects the personality and integrity of the individuals, the groups, and the organizations. He knows that every intrusion to individuality by use of health data, without authorization and consent, constitutes a serious and continuous threat of possible exploitation of individuals, groups, and populations.

Individual integrity

The h.i. maintains personal integrity to a high level, which is fundamental for the harmonious development and fulfilment of the purposes of the health organizations and of the society. The individual integrity includes characteristics which create a feeling of pride to the h.i. Such characteristics are honesty, goodness, objectivity, sensitivity for others, and trust in human relations. He does not give false impressions, regarding the possible abuse of the data processing systems.

Professional competence

The h.i. has consciousness of his personal responsibility to maintain and update constantly his technological competence, within the changing domain of information systems which are based on computers. He is aware of the possibilities and restrictions of his specialization in the area of health and in the more general area of data processing as well.

Personal responsibility

The h.i. undertakes personal responsibility for whatever he contributes in the domain of health. He undertakes tasks only when there are logical hopes that he will be able to respond to them. During the course of the tasks he undertakes, he provides information to the interested parties. He contributes to the objective control and assessment of the effectiveness of the information systems which he uses, in order to attain the socially acceptable purposes which are envisioned.

ORGANIZATIONAL ETHICS

Standards of High Performance

Given the ample support of the health organization, in which he operates, the h.i. exploits, to the full, the resources available to him, in order to achieve internationally recognized standards of high performance, which he expands and specializes in his work. In order to achieve this goal, the h.i. also aims at the interconnection of the health organization he serves, with the proper organizations in the country and abroad.

Legal Protection

The h.i. respects the national legal framework in which he operates, protecting his work from computer crime.

Productivity and quality of working environment

The h.i. creates a working environment of high quality, aiming at the increase of his productivity to the benefit of the health of the society and himself.

Users' participation and feedback

The h.i. aims at the maximum possible participation of users, during the design of health information systems, so that the latter enjoy the maximum possible approval. He reconsiders the results of his activities, so that every new design of a health information system required constitutes as improvement over the one already existing.

INTERNATIONAL LEGAL ETHICS

International intellectual property

The h.i. respects the regulations of the international rules on intellectual property of software, hardware, communications and in general of every form of computer product, recognizing these as a consequence of investment in relative scientific and technological creation. However, he maintains the right to put in front the regulations which apply to his specific national environment.

International Public Law

The h.i. respects and recognizes[5] the social obligations which are connected to the health informatics, as these result from the international public law and regard nursing institutions, multinational organizations, supplying companies and social groups.

International law on telecommunications

The h.i., in the framework of the international law on communication, uses the capabilities of the telecommunications deservingly to the benefit of the society's health.

International Penal Law

The h.i. recognizes, according to the international penal law, as crimes in this domain the abuse of the health information systems, the implanting of program-viruses in them, software piracy, software and hardware theft, fraud, and embezzlement through intervention in computers and sabotage of health information systems.

INTERNATIONAL ETHICS OF PUBLIC POLICY ON HEALTH

Freedom of Communication of Health Data

The h.i.[6] receives and transmits health data when the improvement of the society's health is served and the individual and social rights are not harmed.

Humanitarian Health Information Systems

The h.i. does not use badly designed systems which can damage health. The health information systems, which he uses, are well designed and do not affect the humanitarianism, the dignity, or the human rights.

International Standards on Health Informatics

The h.i. uses, when necessary and to the maximum possible, the international standards[7] of health information systems, contributing also himself to them, with his own knowledge.

Equal opportunities in the health informatics' services

The h.i. recognizes the enormous differences between the developed and the underdevelopment countries, with regard to health informatics' services. In the measure of his capabilities, he contributes with his own initiative or when he is asked by the proper authorities for diminishing these differences.

Individuality and Human Rights

The h.i. absolutely respects the individuality and the human rights which depend on the use of the health information systems and every act of his results from this respect.

Quality of life

The h.i. respects the natural and cultural environment in which he operates and the promotion of the quality of life through health is based on the maintenance of the cultural and natural inheritance.

---

[1] The text which was provided has been slightly edited according to the recommendations of the Publisher.

[2] GRITZALIS D., TOMARAS A., KATSIKAS S., KEKLIKOGLOU J., Data security in Medical Information System: The Greek Case. *Computers and Security*, 10(2): 141-159, 1991.

[3] The Greek-Data Protection Bill (draft), 1988 (in Greek).

[4] There is presently a Working Group on HIDEC within the CEC AIM/SEISMED (Secure Environment for Information systems in MEDicine) Programme. (Contact: Prof. Herman NYS, Centre for Biomedical Ethics and Law, KU-Leuven, Kapucijnenvoer, 35, B. 3000 LEUVEN)

[5] The text which has been provided inserts here a 'in mutual base' which could mean most probably: 'whereas there is a mutual agreement'! *Note of the Editor.*

[6] *Idem.*

[7] The text uses the term 'reference' as in the expression 'terms of reference'. We have preferred 'standards'. *Note of the Editor.*

Japan Information Service Industry Association (JISA) Code of Ethics and Professional Conduct

English translation provided in November, 1993

Aiming at high and reliable position in the Japanese industry, every member of the Japan Information Service Industry Association (JISA) has committed itself to abide by the following code[1].

1. GENERAL DECLARATION

Every member company should realize the mission of the information service industry and fulfil its social responsibility not only to the region it belongs to, but also to society as a whole.

2. BUSINESS CONDUCT

Every member company should understand that its prosperity could be inseparably linked to its clients and make every effort to win their confidence of partnership by:

1) entering into a contract with clear and exact terms and implementing them faithfully.
2) strictly adhering to the client's need to keep its project, its strategies, and any other related information confidential.
3) and constantly providing the clients with quality service.

3. INTERNAL IMPERATIVES

1) Member companies should not make trouble to other member companies by acting against the rules of competition.
2) Member companies should not hire an employee away from another member company in order to gain confidential information and/or win away a contract.
3) Member companies should strictly abide by the law and any contacts entered into regarding intellectual property rights.
4) Member companies should participate in the association's activities as often as possible in order to exchange technology and experience, and raise the level of the whole industry.
5) Member companies should make every effort to provide a satisfactory work environment for their employees, as well as provide them with good and safe working conditions.

[1] 'The predecessor of JISA was established in 1970, and new companies have joined JISA every year since. In August 1993, there were 650 member companies, including 84 supporting members. JISA conducts domestic and international activities aiming at its promotion in the Japanese Industry.' *Letter to the Editor.*

6) Member companies should try to develop their employees' technological faculties, to help them cultivate themselves and to teach them to have pride in their work and professional conduct.

VRI (Vereniging van Registerinformatici) Code of Ethics[1]

PREAMBLE

The Code of Ethics of the VRI (the Dutch Association of Information Scientists) has been developed to serve as an evolving framework for the thinking, acting and testing of persons, who want to be recognizable as RIS (Registered Information Scientists) in their occupational performance in the field of informatics.

The VRI thinks that the RIS in applying this Code contributes to a constructive development and application of informatics.

CODE

In my role as an information scientist I will constantly positively serve the interests of society in all its aspects. I have therefore registered myself in the Register of the Information Scientists. I hereby indicate that I would like to be publicly recognized as such and will at all times be answerable for having followed the Code of Ethics.

RULES OF CONDUCT

1. The RIS should be recognizable as such at all times.
2. The RIS should be aware of the consequences of his acts for society.
3. In his professional activities the RIS should act in accordance with the interests of his employer.
4. The RIS should constantly aim at providing and/or achieving high standard services, contributions or results.
5. The RIS should treat data, obtained within the framework of the assignment, confidentially and may only use these for the purpose for which they were given.
6. The RIS should act within the framework of the assignment in such a way that his procedure may be examined at all times.
7. The RIS should act in such a way that the prestige of his profession and that of his colleagues remains unharmed.
8. The RIS should not (co)operate in bringing about information systems, the application of which could deliberately harm persons, institutions or the public interest or which are against the law.
9. The RIS should be aware of the limits of his knowledge and skill in his occupational performance.
10. The RIS must at all times keep himself informed of developments in the field in which he profiles himself as an expert.

COMMENTS ON THE RULES

1. The RIS should be recognizable as such at all times

The application of informatics is still increasing. As a consequence the information scientist is involved in a growing number of developments.

---

[1] Text received in October 1993.

It is therefore important to know in which way an information scientist applies his knowledge and skill and whether he has committed himself explicitly to act in accordance with standards and rules.

Since the RIS has committed himself to follow previously set standards of quality and integrity, he should be recognizable as an RIS by those he is involved with. The importance of recognizability has not only a positive significance as meant previously, but can also be related to negative situations.

If an RIS does not behave in accordance with the Code of Ethics one should be able to call upon him with reference to the obligations his entry in the Register of information Scientists imposes upon him.

Anyone who thinks the RIS is not acting in accordance with the Code of Ethics may settle the dispute before the arbitration court of the VRI.

2. *The RIS should be aware of the consequences of his acts for society*

Application of informatics and therefore the work of the RIS brings about fundamental changes in society in general, and organizations in particular. By implementing information systems, working conditions, organization and cooperations will change.

Adjustments of duties and responsibilities of employees are often taken into consideration. Corollaries of this, with regard to the prestige of the work in question and the changes in the social position of those involved, are often not taken into consideration or even recognized.

The RIS must also include these aspects in designing information systems. Likewise the RIS should be aware of the possible abuse of the information system he is designing. The possibility that an application will be used differently from the way it was meant may be reason enough not to develop that application nor have it developed.

To prevent application of technologies having too much an autonomous character, much attention must be given to the effects that can be expected. On the other hand, the RIS must be very much aware of situations in which application of information technology may bring about improvement in circumstances, persons, organizations or society. Encouraging applications is also part of the ethics of the RIS. In all circumstances it is of great importance that the RIS is explicit in his considerations whether or not to contribute to, or to initiate the development of information systems.

3. *In his professional activities the RIS should act in accordance with the interests of his employer*

The RIS is engaged by his employer as an expert.

Through lack of time, knowledge, skill, quality or any other reason, the employer himself is not able to serve his interests sufficiently. Therefore the RIS will advise and actively support so he can make the right decision himself at a given moment. Should the employer act or decide contrary to the advice of the RIS, then the RIS must make explicit the consequences of not following his advice.

4. *The RIS should constantly aim at providing and/or achieving high standard services, contributions or results*

In return for his money, every employer expects a product or a service in agreement with his expectations. The RIS, therefore, is obliged to define requirements as to the quality and measure points. As testing afterwards can only lead to approval or disapproval, the RIS must constantly be aware of the quality aspect.

In this way possible uncertainty of employers caused by much negative publicity can be diminished or removed entirely.

In spite of the fact that the quality aspect will initially only lead to an increase of the development costs the explicit requirements as to quality will therefore often be absent, the RIS must do his utmost to emphasize the quality aspect to the employer and to point out the long-term effect of a decrease in the running costs.

In this way something is supplied which will also meet the expectations of the employer in the long run.

5. *The RIS should treat data, obtained within the framework of the assignment, confidentially and may only use these for the purpose for which they were given*

The nature of the duties of an RIS often involves examination of and/or access to data

considered confidential by the owners or by those to whom the data refer.

It is ethically irresponsible towards people and institutions to use these data for other purposes than they were supplied for, or to treat them carelessly so that a third party could use or abuse these data.

By taking the utmost care the RIS can gain or enlarge the trust with regard to the registered information scientist.

Even when aspects of privacy do not seem to apply or seem exaggerated the RIS must, in view of the above, treat all data supplied as confidential.

6. *The RIS should act within the framework of the assignment in such a way that his procedure may be examined at all times*

When a project starts the final result will generally be known. From this can be concluded what final products must be accomplished to achieve this.

When the assignment is finished the result can be compared to the previously defined requirements and discharge could follow. However, it still happens much too often that (large scale) information projects fail, partly due to the fact that the interim evaluation did not or could not take place.

That is why the rule wants to indicate that proceedings must be verifiable not only at the end of the assignment but during all stages of its completion.

In this way the employer or client will not be faced with unpleasant surprises and the employer or client will be invited to participate in the process.

Testing will require certain criteria.

These can consist of (interim) results previously agreed upon or standards that prescribe how the job needs to be done. In accordance with this, the extent to which the RIS has contributed to the effectuation of the result can be judged.

The authorities, society or the RIS colleagues must be able to verify his work if necessary. In all openness, without the RIS hiding behind technicalities or jargon.

7. *The RIS should act in such a way that the prestige of his profession and that of his colleagues remains unharmed*

The statements, attitude and behaviour of the RIS are inspired by dignity, sincerity and integrity in such a way that a harmonious functioning in exercising his profession is achieved.

Among other things this is reflected in dealing responsibly with the risks of informatics as well as in charging socially accepted tariffs.

8. *The RIS should not (co)operate in bringing about information systems, the application of which could deliberately harm persons, institutions or the public Interest or which are against the law*

Before an RIS accepts an assignment he has to assure himself of the preconceived objectives of the product or service that will result.

Apart from general social standards, his own ethical standards are important too. As to the public interest not every RIS will apply the same standards.

However, he should at all times be aware of the effects that result from his professional activities and he must be able to justify these.

9. *The RIS should be aware of the limits of his knowledge and skill in his occupational performance*

The field of informatics knows many disciplines. The RIS will only master one or just a few of them. Whenever the RIS has to go beyond the limits of his professional knowledge or even the limits of the profession itself, he should not hesitate to call upon other specialists.

The RIS may, of course, be asked to go beyond the limits of his professional knowledge or he may suggest this himself. In this way the RIS is able to enlarge his knowledge or skill.

Explicit agreement with the employer and other parties involved must then be obtained.

10. *The RIS must at all times keep himself informed of developments in the field in which he profiles himself as an expert*

Developments in the fields of computer science, methods and technologies for the designing of information systems and the market of those who provide services, change rapidly.

After initial training and education the knowledge of an information scientist soon lags behind. Besides this there are experiences of others with means and methods the information scientist must be able to pass on to interested parties.

A permanent education is necessary to retain an ability to judge the importance of new developments and where and how they can be applied.

DEFINITIONS

Informatics is the field in which one occupies oneself with the automation of information systems and all related fields, such as technology and social, administrative and industrial organizations, man and society.

The term *information scientist* refers to anybody who works in the field of informatics.

The term *RIS* refers to every person who has been registered in the Dutch Register of Information Scientists.

The term *information system* refers to the entire body of systematically collected, recorded, processed, reproduced and provided data in any form, in order to obtain information.

An *employer* is an individual or a legal person who gives the assignment to supply services and products.

The *client* is he who uses the services or products supplied by the information scientist.

Secretariaat VRI, Postbus 63
1243 ZH 's-Gravenland, The Netherlands
Phone: +31/35-62262; Fax: +31/35-64073

Code of Ethics of the Dutch Association of Information Scientists. A short Comment

Jan HOLVAST
Holvast and Partner
Privacy Consultancy, Landsmeer
The Netherlands

INTRODUCTION

Codes of conduct and codes of practice are a generally accepted phenomenon in the Netherlands. They are sometimes used as an alternative or supplement to legislation. An example of the latter is the assumption of self-regulation in the area of protection of privacy, which is seen as one of the main characteristics of the Dutch Privacy Protection Act.

There are two codes in the area of information technology which are seen as alternatives to legislation. The first is the code of the Dutch Association of Information Scientists (VRI). The second is the code of the Dutch Chartered Informaticians. I will only comment now on the first code.

PROFILE AND CONSTITUTION OF THE ASSOCIATION

In contrast to the Dutch Society of Informatics (NGI), the Dutch Association of Information Scientists is a rather young and more limited organisation. Established in 1984, it has at the moment approximately 2,500 members.

The aim of the Association is to improve the quality of work of those who work on a professional basis in Information Science. An important tool in achieving this aim is the Code of Conduct.

MEMBERSHIP STRUCTURE

Members have to be information scientists and must be recognised Registered Information Scientists (RIS), inscribed in a register. Only individuals who have been accepted by a Chamber of Acceptance may be registered. Two criteria must met to be accepted: education and experience. A scientific training in information science, as well as at least six years of experience as an information scientist, are required. The code is directed towards the individual conduct and behaviour of the RIS.

RULES AND RESPONSIBILITIES

The general nature of the code is one that is rather general and not detailed. It consists of ten general statements preceded by a preamble.

Although not stated implicitly in the Code, the status of the code starts with a kind of pledge. "In my role as an information scientist, I will constantly positively serve the interest of society in all its aspects. I have therefore registered myself in the Register of the Information Scientists. I hereby indicate that I would like to be publicly recognised as such and will at all times be answerable for having followed the Code of Ethics."

In the Rules of Conduct, these responsibilities are more or less repeated: "The RIS should be aware of the consequences of his/her acts on society."

HOW THE CODE HAS WORKED OUT

The code of Conduct is, for a large part, directed at the method of working. It is expected that four general rules are applied:

- the information scientist's pronouncements, actions, and discussions should be in accordance with his/her experience;
- the information scientist should carefully guard the confidentiality and integrity of (personal) data;
- the information scientist should strive to prevent improper use and misuse of means and systems;
- the information scientist should be aware of the fact that his/her work results in fundamental changes in an organisation.

RULES OF ENFORCEMENT

The Association has a Conciliation Board which deals with complaints against individual members. One sanction may be the removal of a member. As far as is known, no such sanction has been effected up until now.

PROCESS OF UPDATING THE CODE

The process of updating can be seen as continuous, during which the more theoretical Code of Conduct is tested through concrete situations, through the content and expectations expressed in legal opinions concerning a case where there is conflict, and through contributions from other professional and organised interest groups working in or together with information science. A special section, the Chamber of Codes, is responsible for these activities. The result may be a refinement of the Code or adoption of new measures.

EDUCATION AND TRAINING IN THE FIELD OF ETHICS FOR THE MEMBERS

Seminars and conferences in which ethics and ethical conduct are important themes are organised on a more or less continuous basis.

Code of Ethics of Information Processing Professionals Association of Korea (IPAK)[1]

[1.1] I take pride in being a member of the Information Processing Professionals Association of Korea, and as a professional I take a thorough responsibility for information system users, my fellow members, my society, my country and even all of mankind,

[1.2] I do my best to enhance the benefits and convenience for users,

[1.3] I love and respect my fellow members for their knowledge, morality and faithfulness,

[1.4] I am ready to cooperate thoroughly in executing efficiently national and society policies,

[1.5] I shall make every effort to ensure that information systems are used to improve the quality of life for all of mankind.

[2] *In recognition of my obligation to my society and country, I shall:*

[2.1] make an effort to keep my information up-to-date for the improvement of society and country and provide appropriate information whenever needed,

[2.2] exclude personal selfishness as well as group selfishness and strive to make fair judgments in case of conflict of interests,

[2.3] protect the proper interests of society and country and strive to keep a fair, honest and objective viewpoint,

[2.4] maintain secrecy and confidentially concerning information acquired,

[2.5] be answerable to history and not provide or stick to any information against the main tide of technology evolution,

[2.6] not use resources of society or country for personal gain or any other purpose with proper legal authorization,

[2.7] not exploit any weakness of the information system and take the initiative in enhancing and improving any such weakness.

[3] *In recognition of my obligation to human society, I shall:*

[3.1] protect privacy and maintain secrecy concerning all information entrusted to me,

[3.2] endeavor to share my skill and knowledge with others around me,

[3.3] make a sincere effort to ensure that my achievements are used in a manner useful to society,

[3.4] make an effort to ensure that information technology is used to improve the quality of life.

---

[1] English translation provided by the Korean Information Society, September 1994. Numbering in [ ] is ours, in order to facilitate the reference in the detailed Tables which are given in the Annexes. *Note of the Editor.*

Standards of Conduct of IPAK

[1] These standards of conduct provide behavior guidelines to facilitate practice of the code of ethics. These standards are minimum practice guidelines for the professionals.

[2] *In recognition of my obligation to the information systems users, I shall:*

[2.1] pursue self-innovation, keeping my knowledge up-to-date and offering my expertise whenever needed,

[2.2] share my information and knowledge with others and provide true and objective information to system users,

[2.3] take full responsibility for my duty and mission,

[2.4] not abuse the rights entrusted to me,

[2.5] not give wrong information about technology and systems, nor misrepresent myself, nor be self-assertive,

[2.6] not exploit the lack of knowledge or inexperience of users about information systems.

[3] *In recognition of my obligation to my society and country, I shall:*

[3.1] act morally in all my professional relationships,

[3.2] take appropriate action in regard to any illegal or unethical practices based on truth and reasonableness without regard to personal interest,

[3.3] do my best to cooperate with the fellow members who lack knowledge and experience,

[3.4] put myself in the others' place at all times and not take advantage of others' lack of knowledge or inexperience,

[3.5] do no harm to my fellow members in any way.

Computer Professionals for Social Responsibility (CPSR) Code of Fair Information Practices[1]

To promote information privacy

Computer Professionals for Social Responsibility (CPSR) and Privacy International

Stop Data Misuse

Personal information obtained for one purpose should not be used for another purpose without informed consent.

Encourage Data Minimization

Collect only the information necessary for a particular purpose. Dispose of personally identifiable information where possible.

Promote Data Integrity

Ensure the accuracy, reliability, completeness, and timeliness of personal information.

Allow Data Inspection

Notify record subjects about record-keeping practices and data use. Allow individuals to inspect and correct personal information. Do not create secret record-keeping systems.

Establish Privacy Policies

Establish and enforce an information privacy policy. Make the policy publicly available.

---

[1] The original Code of Fair Information Practices was published in the 1973 Report of the Department of Health, Education, and Welfare, entitled 'Computers, Records & the Rights of Citizens'. Many organizations, including CPSR and Privacy International, have reprinted, modified, or adapted the Code.

Computer Professionals for Social Responsibility (CPSR) Code of Fair Information Practices for the National Information Infrastructure (NII)[1]

CPSR believes that an NII privacy code should be developed and enforced. We have already recommended a set of principles that could help address many of the privacy concerns the NII will raise. These principles are as follows.

1. The confidentiality of electronic communications should be protected.
2. Privacy considerations must be recognized explicitly in the provision, use and regulation of telecommunication services.
3. The collection of personal data for telecommunication services should be limited to the extent necessary to provide the service.
4. Service providers should not disclose information without the explicit consent of service users. Service providers should be required to make known their data collection practices to service users.
5. Users should not be required to pay for routine privacy protection. Additional charges for privacy should only be imposed for extraordinary protection.
6. Service providers should be encouraged to explore technical means to protect privacy.
7. Appropriate security policies should be developed to protect network communications.
8. A mechanism should be established to ensure the observance of these principles.

---

[1] Marc ROTENBERG, Privacy and the National Information Infrastructure, in: *EDUCOM*, Vol. 29, No. 2, March/April 1994, pp. 50-51. This short code is reproducing the eight principles which were already mentioned in the 1992 'Proposed Privacy Guidelines for the National Research and Education Network'. We reproduce the 1992 text, with the kind permission of the author, as a developed explanation of these eight principles.

Proposed Privacy Guidelines for the National Research and Education Network

Statement of Marc ROTENBERG[1]
Washington Director
Computer Professionals for Social Responsibility (CPSR)

Thank you for the opportunity to testify today before the National Commission on Library and Information Science (NCLIS). My name is Marc Rotenberg and I am the Director of the Washington Office of Computer Professionals for Social Responsibility (CPSR). CPSR is a national organization of professionals in the computing field. I would like to speak with you about privacy protection and the future of the NREN. This is item 6 identified in the NREN research agenda.

Richard Civille will speak with you next about CPSR's work to promote Local Civic Networks. During the past few years CPSR has coordinated several national efforts to promote privacy protection for network communication. From cryptography to Caller ID, we have sought to ensure that the rapid developments in the communications infrastructure do not diminish the privacy we all value.

We believe that the future of network communications depends largely on the ability to make certain that sufficient privacy protection is available for all users of the network. In this effort we have worked closely with the library community. It became clear to us that library organizations have a special appreciation for the importance of privacy protection. For many, privacy is the critical safeguard that protects intellectual freedom and promotes the open exchange of information. The American Library Association, the Association of Research and other library organizations have all shown their support for privacy protection through codes of conduct, policy statements, and research conferences.

We have also worked closely with telecommunication policy makers in the United States and around the world. The New York state Public Service Commission issued a policy on telecommunication privacy which set out several principles for network communications. These recommendations have been followed in several states. More recently, the Minister of Communications in Canada issued a series of principles on communications policy.

---

[1] Open Forum on Library and Information Service's Roles in the National Research and Education Network (NREN), National Commission on Libraries and Information Science (NCLIS), Washington, DC, July 22, 1992.

Meanwhile, the Commission of the European Communities has put forward a draft directive on Data Protection in Telecommunications.

The European Commission made a critical point about future network development. It said that 'the effective protection of personal data and privacy is developing into an essential precondition for social acceptance of new digital networks and services.' This view is shared by agencies in other countries that have looked at the implications of advanced networking services. For example, the Ministry of Posts and Telecommunications in Japan recently concluded a study on the protection of personal data in the telecommunications business and recommended a series of privacy guidelines to accompany the introduction of new network services.

In the United States, however, we find ourselves in the midst of the greatest privacy debate in a generation. In the absence of a coherent federal policy to protect privacy, consumers have been left to fend for themselves, and the response is not encouraging. From Pennsylvania to California, telephone companies now face widespread and well-founded consumer opposition to new telephone services. Part of the reason for this is that there has been little effort in the United States at the federal level to develop privacy principles for new network services.

CPSR would like to see an agency in the United States take on the task of developing and promulgating privacy principles for network services. We have already recommended the creation of a data protection board which could, among other tasks, develop appropriate principles for network communications. There is a proposal before Congress to establish such an agency, but is unclear whether it will be enacted this year.

Meanwhile, the Federal Communications Commission (FCC) has been unwilling to address the privacy implications of new network services. We are also somewhat disappointed that neither the Computer Science and Technology Board (CSTB) of the National Research Council or the Office of Technology Assessment (OTA) has addressed privacy concerns for network users. Both the CSTB and the OTA are well qualified to tackle this problem.

In the interim, NCLIS could take a leadership role, and help develop and promulgate privacy principles for the emerging communications infrastructure. It is clearly in the interest of the library and information science community to ensure adequate privacy protection, but unless some agency takes on this responsibility it appears unlikely that the work will be undertaken.

CPSR believes that it is in the long-term interest of our country and of computer users around the world to ensure protection for networked communication. The failure to develop such policy may impose very high costs on all network users, and may ultimately reduce greatly the value of the network to users.

Speaking academically, the absence of adequate protection for electronic communication is a substantial gap in NREN policy that should soon be addressed if the full potential of the infrastructure is to be realized. Speaking practically, if we don't get some good policy soon, we may all be buried in a blizzard of electronic junk mail the likes of which we have never known.

I would like now to make three points about the current state of privacy protection for NREN, and then propose a series of principles for privacy protection. These principles may help 'get the ball rolling' and encourage the development of other initiatives. I hope that

NCLIS will recommend that the Office of Science and Technology Policy (OSTP) give these principles full consideration.

FINDING 1:

Commercialization of the NREN will exacerbate existing privacy problems. Without a clear mechanism to protect privacy, user concerns will increase. Much of the discussion surrounding the NREN today focuses on the opportunity to develop commercial services and to provide network access for private carriers. We do not oppose efforts to provide commercial services. Clearly, there is an important opportunity to develop new services and to offer products through the network. At the same time, it is apparent that the commercialization of the NREN will create new pressures on privacy protection.

In the current network environment, made up primarily of researchers and scientists, there is little incentive or opportunity to gather personal data, to compile lists, or to sell personal information. This is likely to change. Once commercial transactions begin to take place on the net, the information environment will resemble a hybrid of credit card and telephone call transactions. Records of individual purchases will be available and will possess commercial value. The NREN community will face a whole new set of privacy issues.

We anticipate that there will be three different types of privacy problems as the NREN continues to evolve. First, as commercial organizations become users of the network, they will gather personal data, and wish to sell lists. The address files for list servers could be sold, and users may find themselves 'subscribed' to lists they have no interest in. These activities will raise traditional privacy concerns about the restrictions on disclosure and secondary use, the opportunity for users to obtain information held by others, and the need to minimize the collection of personal information.

Second, efforts to promote competitiveness in the delivery of network services may also lead to the disclosure of network data which will compromise user privacy. This problem is already apparent in the current rules for the operation of the telephone network. The Federal Communication Commission requires telephone companies to provide records of customer phone calls to other companies so that competing companies may analyze calling patterns and sell their services. Large companies objected to the disclosure of this sensitive information. As a result the FCC required that telephone companies obtain authorization before releasing these numbers. But this restriction only applies to telephone customers with more than 20 lines.

The disclosure of Customer Proprietary Network Information (CPNI) has already surprised many telephone customers who now receive calls from companies with whom they have no prior relationship. These companies are able to describe the customer's telephone calling habits in great detail. Users of NREN services are also likely to object to the disclosure of network information.

The third problem is that law enforcement agencies are likely to make 'greater demands' on communication service providers to turn over records of electronic communications to the government and to provide assistance in the execution of warrants. I say 'greater demands' with some reservation since the recent proposal from the Federal Bureau of Investigation to require that all communications equipment in the United States be capable of wiretapping seems about the greatest demand conceivable. Still, we should anticipate that the government demands for access to the contents and records of NREN communications are likely to increase.

FINDING 2:

Current privacy protections are inadequate. Electronic communications are provided some protection against unlawful interception by the Electronic Communications Privacy Act (ECPA) of 1986. This law extends the very important guarantees contained within the 1968 wiretap statute to digital communication and stored electronic mail. But this protection now appears inadequate. As a general matter, the wiretap law protects the contents of an electronic message against unlawful disclosure; it does not protect the record of the transaction against disclosure.

ECPA also does not appear to protect critical personal information, such as a person's telephone number, from improper disclosure. For example, the Calling Number Identification (CNID) service is probably a violation of the wiretap statute and clearly a violation of the wiretap law of several states. Nonetheless, the service has been offered over the objection of consumer groups, technical experts, and legal scholars.

FINDING 3:

Technical safeguards provide only a partial solution. There are some in the network community who believe that technology will provide a solution to these emerging privacy problems. New techniques in cryptography provide ways to protect the contents of an electronic message and even to protect the identity of the message author. An article that will appear next month in Scientific American entitled 'Achieving Electronic Privacy' describes in more detail how it may be possible through technical means to recapture some privacy.

CPSR has supported many efforts to improve technical means for privacy protection. In fact, CPSR has been one of the leading proponents of the widespread us of cryptography to protect electronic communications. We have opposed restrictions by both the National Security Agency and the Federal Bureau of Investigation on the use of cryptography. We have also supported the development of privacy-enhancing technologies, such as telephone cards which are widely used in Europe and Japan, and recommended that policy makers explore technical means to protect information.

Nonetheless, we do not believe that technical safeguards will provide sufficient protection for networked communications. Our right of privacy is based on Constitutional principles and our national history, and reflects our commitment to certain political ideals. The protection of privacy is ultimately a policy decision that must be resolved through our political institutions. Clearly, technology provides useful developments that we should incorporate into future networks, but it would be a mistake to assume that technology alone will provide sufficient protection.

This point was made two decades ago by former White House Science Adviser Jerome Wiesner who also served as president of MIT. In testimony before Congress on the privacy implications of data banks, Professor Wiesner said:

> *There are those who hope new technology can redress these invasions of personal autonomy that information technology now makes possible, but I don't share this hope. To be sure, it is possible and desirable to provide technical safeguards against unauthorized access. It is even conceivable that computers could be programmed to have their memories fade with time and to eliminate specific identity. Such safeguards are highly desirable, but the basic safeguards cannot be provided by new* inventions. *They must be provided by the legislative and legal systems of this country. We must face the need to provide adequate guarantees for individual privacy.*

We believe that the development of NREN privacy policy should be conducted in this spirit: looking for opportunities to incorporate technical safeguards while recognizing that the ultimate decisions are policy-based.

PRIVACY GUIDELINES:

Before discussing the proposed privacy principles, I would like to say a few words about the desirability of developing these principles. Privacy protection in electronic environments is a particularly complex policy problem. There is legal jargon and technical jargon. There are rapid changes. And there are certainly a wide range of opinions about how best to achieve privacy, even about what privacy means.

Privacy principles have helped to clarify goals and to convey objectives in non-technical terms. Well developed polices are 'technology neutral' and are adaptable as new technologies emerge. Professional organizations have made widespread use of such principles for codes of ethics and for public education.

There are a number of such polices in the privacy realm. Some of these polices have been extremely influential in the development of public policy, national law, and international agreements. For example, the Code of Fair Information Practices was the basis for the Privacy Act of 1974, the most extensive privacy law in the United States. The Code was developed by a special task force created by the Secretary of Health, Education, and Welfare in 1973. Other codes have formed the basis for data protection law in Great Britain.

All of these codes seek to establish certain responsibilities for organizations that collect personal information, and to create certain rights for individuals. In developing these telecommunication privacy guidelines, we examined existing codes and particularly the principles developed by the Organization for Economic and Cooperative Development (OECD) in 1981. We also incorporated several additional principles that we believe are necessary to protect personal information in communication environments. Taken as a whole, the principles are intended to improve privacy protect ion for network communications as the NREN continues to evolve.

RECOMMENDATION 1:

The confidentiality of electronic communications should be protected. The primary purpose of a communication network is to ensure that information can travel between two points without alteration, interception, or disclosure. A network that fails to achieve this goal will not serve as a reliable conduit for information. Therefore the primary goal should be to guarantee the confidentiality of electronic communications.

RECOMMENDATION 2:

Privacy considerations must be recognized explicitly in the provision, use and regulation of telecommunication services. The addition of new services to a communications infrastructure will necessarily raise privacy concerns. Users should be fully informed about the privacy implications of these services so that they are able to make appropriate decisions about the use of services.

RECOMMENDATION 3:

The collection of personal data for telecommunication services should be limited to the extent necessary to provide the service. Users should not be required to disclose personal data which is not necessary for the rendering of the service. In particular, the use of the Social Security number should be avoided. In no instance, should it be used as both an identifier and authenticator.

RECOMMENDATION 4:

Service providers should not disclose information without the explicit consent of service users. Service providers should be required to make known their data collection practices to service users. Service providers have a responsibility to inform users about the collection of personal information and to protect the information against unlawful disclosure. Personally identifiable information should not be disclosed without the affirmative consent of the user.

RECOMMENDATION 5:

Users should not be required to pay for routine privacy protection. Additional costs for privacy should only be imposed for extraordinary protection. The premise of the federal wiretap statue is that all users of the public network are entitled to the same degree of legal protection against the unlawful disclosure of electronic communications. This principle should be carried forward into the emerging network environment. Segmented levels of privacy protection are also likely to introduce new transaction costs and create inefficiencies. Where special charges are imposed for privacy, it should be for 'armored car' service.

RECOMMENDATION 6:

Service providers should be encouraged to explore technical means to protect privacy. Service providers should pursue technical means to protect privacy, particularly where such means may improve the delivery of service and reduce the risk of privacy loss.

RECOMMENDATION 7:

Appropriate security polices should be developed to protect network communications. Security is an element of privacy protection but it is not synonymous with privacy protection. Appropriate security policies should be put in place to protect privacy. However, it should be recognized that some security measures may compromise privacy protection. Network monitoring, for example, or the collection of detailed audit trail information will raise substantial privacy concerns. Therefore, security policies should be designed to serve the larger goal of privacy protection.

RECOMMENDATION 8:

A *mechanism should be established to ensure the observance of these principles.* Good principles without appropriate oversight and enforcement are insufficient to protect privacy. This has been the experience of the United States with the Privacy Act of 1974 and of the European countries with the OECD principles of 1981. In both instances, fine principles lacked sufficient oversight and enforcement mechanisms.

Additional principles may be appropriate and these principles may well need modification. But we hope that they will provide a good starting point for a discussion on communications privacy for the NREN.

American Society for Information Science (ASIS) Code of Ethics for Information Professionals

ASIS recognizes the plurality of uses and users of information technologies, services, systems and products and the diversity of goals or objectives, sometimes conflicting, among vendors, producers, mediators, and users of information systems. ASIS mandates high standards for its members, identifying the following areas of responsibility:[1]

RESPONSIBILITY TO EMPLOYERS / CLIENTS / SYSTEM USERS

[1][2] To act faithfully for their employers or clients in professional matters;

[2] To uphold each user's, provider's or employer's rights to privacy and confidentiality and shall respect whatever proprietary rights belong to them:

[2.1] by minimizing data collected about clients, patrons, or users, and by limiting access to, providing proper security for and ensuring proper disposal of such data insofar as it does not conflict with the proper goals and constraints of their organizations,

[2.2] by not disclosing information obtained during confidential interviews, except when such disclosure is mandated by law or in accord with proper policies of their employers or the proper rights of their clients.

[3] To treat fairly all persons regardless of race, religion, sex, sexual orientation, age or national origin.

RESPONSIBILITY TO THE PROFESSION

[4] To truthfully represent themselves and the information systems which they utilize or which they represent:

[4.1] by not knowingly making false statements or providing erroneous information or fail to inform clients, sponsors, or employers of the limitations, conditions and constraints of the system,

[4.2] by informing their employers, clients or sponsors of any circumstances that could lead to a conflict of interest,

[4.3] by not using their position beyond their authorized limits or by not using their credentials to misrepresent themselves.

[5] To be and to remain competent and qualified, and to foster competence and deter incompetence among fellow professionals:

[5.1] by only undertaking assignments for which they are qualified, and for which there is reasonable expectation of meeting requirements in a timely fashion,

[5.2] by following and promoting standards of conduct in accord with the best current practices,

[5.3] by undertaking their research conscientiously: in gathering, tabulating or

---

[1] Proposed Revision by Thomas J. FROEHLICH. Current Draft before Board, February, 1992. Dedicated to the Memory of Diana WOODWARD.

[2] Numbering in [ ] is ours, in order to facilitate the reference in the detailed Tables which are given in the Annexes. *Note of the Editor.*

interpreting data; in proper approval procedures for human subjects; or in producing or disseminating research results,

[5.4] by seeking, accepting and offering honest criticism of their work and by pursuing ongoing professional development and by encouraging colleagues and professionals to do the same,

[5.5] by performing services in a manner that enhances or does not discredit the profession,

[5.6] by adhering to principles of due process and equality of opportunity in peer relationships or personnel actions.

RESPONSIBILITY TO SOCIETY

[6] To improve, to the best of their means and abilities, the information systems in which they work or which they represent:

[6.1] by resisting all forms of censorship, inappropriate selection and acquisitions policies, and biases in information selection, provision and dissemination and by striving to correct errors or remedy biases and inaccuracies in information systems,

[6.2] by making known any biases, errors and inaccuracies which exist and can not be or have not been remedied,

[6.3] by providing the most reliable and accurate information and the degree of credibility of the sources as known or unknown.

[7] To promote free and equal access to information, within the scope permitted by their organizations or work, and to resist procedures that promote discriminatory practices in access to and provision of information:

[7.1] by seeking to extend public appreciation and awareness of information availability and provision and the role of information professionals in providing such information,

[7.2] by freely reporting, publishing or disseminating information, subject to legal and proprietary restraints of vendors, producers and employers, and the best interests of their employers, or clients.

[8] Information professionals shall engage in principled conduct whether on their own behalf or at the request of employers, colleagues, clients, agencies or the profession: unprincipled conduct shall be challenged or disclosed.

Draft Code of Ethics

Hal SACKMAN (1990)

PREAMBLE

The IFIP Code of Ethics has been constructed not only for individual Information Technology (IT) professionals, but also for multinational IT organizations, and the extended IT community concerned with international legal informatics and related public policy. This Code provides guidelines for individuals, international organizations, national societies, and those influencing international public policy. The guidelines are global and multicultural, and are not intended to reflect any particular ideology or creed. It is hoped that the evolving Code will contribute to the constructive development and application of Information Technology throughout the world.

1. INDIVIDUAL PROFESSIONAL ETHICS

1.1. Social Responsibility

IT professionals strive to use their technical expertise to advance international human welfare and the quality of life for citizens of all nations. They accept the ethical obligation to assess social consequences and help ensure safe and beneficial use of IT applications.

1.2. Protection of Privacy

IT professionals respect the privacy and integrity of individuals, groups, and organizations. They believe that computerized invasion of privacy, without informed authorization or consent, is a continuing threat for individuals and groups. Public trust in informatics is based on vigilant protection of established ethical standards of information privacy.

1.3. Individual Integrity

IT professionals maintain high standards of personal integrity which are basic for the harmonious integration of organizations and society. Individual integrity encompasses desirable traits such as: honesty, probity, objectivity, sensitivity to others, and trustworthiness in human relations. IT professionals respect and defend the free inquiry of their associates. They do not misrepresent capabilities of information processing systems for their personal gain.

1.4. Professional Competence

IT professionals continually maintain and upgrade their competence in the swiftly changing world of computer-based information systems. They understand the capabilities and limitations of their specialized expertise, and the general field of information processing.

1.5. Personal Accountability

IT professionals accept personal responsibility for agreed expectations concerning their role and work. They accept assignments only when there are reasonable and informed expectations of successfully meeting requirements. They attempt to keep all involved parties -- co-workers, management, clients and users -- properly informed on the progress and status of their tasks. IT professionals objectively test and evaluate information system effectiveness to certify beneficial applications.

2. INTERNATIONAL ORGANIZATIONAL ETHICS

2.1. High Performance Standards

Multinational organizations are aware of their social responsibilities to provide quality goods and services from computer-based information systems and networks. The pursuit of performance excellence, particularly in system reliability and tested system effectiveness, is indispensable for quality information system services.

2.2. International Standards and Regulations

International IT organizations foster international progress by actively contributing to the development of acceptable international IT standards, and in following established regulatory standards. IT multinational organizations are aware that successful globalization of computer-communications networks and beneficial international information services requires the good-will and voluntary concurrence of host governments, competitors, professional informatics societies, and other stakeholders, especially end-users.

2.3. International Legal Protection

In pursuing constructive ethical objectives, multinational IT organizations require legal protection. Such protection includes general legal safeguards such as protection against unfair competition. It also includes protection against computer crime, and intellectual property protection. Multinational organizations conform to the laws of their host countries and established international law pertaining to their operations.

2.4. Employee Productivity and Quality of Working Life

IT organizations strive to improve information systems to enhance the quality of working life for employees. Such enhancements facilitate individual and organizational productivity. These improvements aim at morally desirable goals; such as, personal development, physical safety, personal dignity and human fulfillment in the computerized workplace. IT employees recognize their obligations to foster ethical management/labor relations based on constructive cooperation and shared trust.

2.5. User Participation and Feedback

International IT organizations encourage harmonious user participation in computer-based information system design and development. The user is an integral part of the total information system, and is the ultimate beneficiary or victim. Integration of user attitudes, training, experience, interests, and needs, should be linked with effective human feedback throughout the entire system development cycle. Cooperative and constructive human feedback is fundamental guarantor of IT social responsiveness.

3. ETHICS FOR INTERNATIONAL LEGAL INFORMATICS

3.1. Intellectual Property Law

The IT community values the creative energy that generates new scientific and technological discoveries for worldwide benefits. This creativity often requires international legal protection for intellectual property in hardware, software telecommunications and related goods and services. Without such protection, desirable long-term investments in IT research and development would be severely constrained to the detriment of the entire world community. Intellectual property protection should be balanced against the free flow of open scientific knowledge in the international public domain.

3.2. International Public Law

The IT community strives to meet the social obligations of international public law. Such laws pertain to interrelations among host countries, government institutions, multinational corporations, workers, suppliers, vendors, competitors, international professional organizations, and affected public groups. In legal informatics, these concerns include privacy law, antitrust law, health and welfare law, and regulatory law, including protection

from harmful environmental pollution linked to IT industrial operations.

3.3. International Telecommunications Law

The IT community is mindful of expanding legal consequences of worldwide computer-based telecommunication networks and associated information services. Numerous legal issues arise from international telecommunication agreements and protocols for future networks. These networks anticipate virtually unlimited bandwidth capacities for multimedia communications, with major social impacts. The facilitation of open and equitable global communications through computerized telecommunications can accelerate international trade, understanding, cooperation, and friendship. The development of international legal informatics serving these worldwide goals is a long-range ethical objective of the IT community.

3.4. International Criminal Law

The proliferation of international computer-based networks has led to the emergence of transnational computer crime, raising new challenges for international legal informatics. These crimes have assumed diverse forms, including computerized international money laundering, racketeering, fraud, information piracy, theft, embezzlement, computer program and data contamination, and sabotage. The IT community unequivocally opposes international criminal use of computers, and endorses vigorous international cooperation and legal countermeasures, consistent with due process, to protect the international public interest.

4. INTERNATIONAL PUBLIC POLICY ETHICS

4.1. Freedom of Communication

The IT community, aware of the rapid growth of international communications and networking, appreciates the social responsibilities of international freedom of communication. Such international freedoms include: open access to computer-based information in the public domain, freedom to hold and express personal and group opinions, and, as indicated in the United Nations Charter on Human Rights, the 'freedom to communicate through any media regardless of frontiers'.

4.2. Privacy and Dignity of Individuals

The IT community endorses the fundamental human rights of privacy and dignity for all individuals using or affected by computer-based information systems. These rights stem from a strong concern that computerized systems should never be harnessed to demean or oppress individuals or groups. The IT community believes that the key safeguard is ethically-oriented system design, such that protection of privacy, and enhancement of personal dignity are key system objectives.

4.3. Humanized Information Systems

The international IT community recognizes the primacy of serving social needs. It also recognizes that rapid computerization has consistently outraced humanization of information services. In particular, poorly designed person/machine interfaces may lead to physical stress syndromes. IT professionals and organizations affirm their obligation to continually humanize computer information systems through internationally accepted techniques and standards. These include ergonomic test, evaluations, and certification of information system hardware, software, communications and user services.

4.4. International Computer Literacy

IT professionals and organizations appreciate the need to promote global computer literacy. The fruits of IT are ultimately only as good as the informed and knowledgeable social use to which they are applied. International educational advances in computer literacy may be the most cost-effective general approach to optimize worldwide computer benefits. The professional IT community encourages global excellence in introductory and continuing education in informatics in schools, universities, the home, and the workplace.

4.5. Equitable Opportunity for Information Services

The IT community is concerned about the growing global gap between the information rich and the information poor, which contributes to worldwide social instability,

particularly between developing and industrialized nations. IT professionals and organizations are dismayed by international trends toward inequitable distribution of computer-based information systems, which reinforces this growing information gap. This problem primarily originates from complex international economic forces which are beyond the scope of this Code of Ethics. Nevertheless, the IT community believes it should conscientiously contribute toward helping to establish a more just and equitable socio-economic international solution.

4.6. Cultural Quality of Life and Human Choice

The IT community notes the penetration of computer-based information services into virtually all walks of life. It is concerned with the powerful social consequences of international computerization on cultural styles and values. It appreciates the priceless human heritage of pluralistic, worldwide cultures. The IT community affirms its dedication to harmonize technological change with the distinctive ethos and quality of life associated with each culture. The IT Community supports the basic right of all individuals to participate in shaping the computerization of their culture and society.

Austrian Computer Society (OCG) Comments on the Draft Code of H. Sackman

The submitted IFIP Text 'Ethics of Computing' as well as the comments added thereto deal with a moral behavioural code and address those active in the field of computing. They share this objective with all other Codes of Ethics of engineering and natural sciences. While the codification of moral behavioural patterns for a profession may be important and desirable, similar efforts with other federations of engineers have shown, that the practical results are mostly quite frustrating. Regulations of that kind exist e.g. in the field of FEANI and for nearly decades for the VDI (Federation of German Engineers). The US Federations of Engineers, too, have such Codes of Ethics. The efforts over many years to arrive at cautious formulations in this field have certainly contributed to the forming of an opinion, but the practical results have been rather limited so far. Despite all these reservations, however, the continuation of careful work with this draft code of ethics seems to be duly justified.

Therefore an especially appointed redaction committee worked out this OCG statement to the IFIP paper.

There is a completely different connection between ethics and information processing or computing, however, which is not directly touched by this Code of Ethics. Thus the OCG plans to establish a working group for this subject.

Strongly simplified and abbreviated, the entire field of information processing can be seen as the final evolutionary step of the occidental claim to a rational understanding of the world. That opens the discussion, however, on the relation between the teachability of virtue, a question raised since the times of the ancient Greeks (Aristotle, Plato and the Greek mathematicians) and the relation between knowledge and rationality on the one hand and moral and

values on the other hand. This question can be found in the dialogues of Plato and has marked the occidental history of thinking in various forms ever since. Value and rationality is an issue still discussed by modern philosophy; but hardly ever in relation to the questions and possibilities of computer science.

Nevertheless, the question of values seems to enter a new stage due to the development of computer science, especially because of the activities concerning artificial intelligence. Dealing in this area of research with formal (computer) models for mental processes, we are prompted to ask, whether a program itself can have ethics and whether these ethics reflect that of the program developer. This is also true, if we assume that any program 'does only what it is programmed for'. This is not the case with program systems anymore, since the single person has lost the clear understanding of what the computer exactly does. This could lead to the question, whether a program can have its own ethics or in what respect we can speak of ethics contained in a program. This direction of thought is followed in the works of Weizenbaum, Dreyfus, Minsky, Simon, Varela, Hofstadter, Dennett, Gardner, Searle, Dretske, Churchland, Ornstein, etc. But even if we do not want to immerse that profoundly, it seems important to inquire further, whether there could be a hidden ethical behaviour in programs if they contain decision structures (e.g. in the fields of medicine, diagnostic programs, etc.).

In principle we have to face the ethical dimension of the question when we advance to exhaust the full potential of computers. Can laws of ethics be expressed in mathematical terms and thus be incorporated in programs? Is there behind that idea the thought of a general, basic and uniform ethics that can be formalized or do we have to accept something like ethic moods or regionally and temporally limited ethical standards? Can programs (rational systems) reflect values or systems of standards? These questions do not seem to be touched by the draft code of ethics. Their discussion would ask for interdisciplinary co-operation beyond this field including in particular philosophers, anthropologists, historians, linguists etc. IFIP could provide the forum for that purpose, should there be enough interest among its members. One of the most desirable results perhaps of such a discussion could be the chance to lead the fields of information processing and computer science beyond their narrow limits of technical science.

Keeping these general remarks in mind, we shall give now some more detailed comments on Prof. Sackman's draft. The comments, resulting from numerous discussions about this topic, will follow the pattern of the draft i.e. the numeration corresponding to the numbers used in the work of Prof. Sackman.

1.1. Social Responsibility

This paragraph is a collection of very high but equally vague moral demands of universal validity, which bear no specific relevance to the subject of Information Technology.

Suggestion: This paragraph to be omitted.

1.2. Protection of Privacy

No comments.

1.3. Individual Integrity

This paragraph asks for moral standards which have no specific bearing on IT or computer technology.

Suggestion: The demands should be restricted to the topic in question. The BCS Code of Conduct, 2.2. 'Professional Integrity' gives a good example for an adequate wording[1].

1.4. Professional Competence

It is doubtful whether a lack of professional competence in itself represents a violation of moral standards. This would be the case only if an individual, despite being aware of his own incompetence, tried to feign capabilities he or she doesn't possess. In this respect also refer to the BCS Code of Conduct.

Suggestion: Adequate change of this paragraph.

1.5. Personal Accountability

The third sentence might contradict national laws and/or contractual agreements between partners and should therefore be omitted. The fourth sentence has nothing to do with a Code of Ethics and should be omitted as well. The paragraph should be replenished by a reference to possible conflicts of interests in order to avoid any prejudice of impartiality. As an example refer to the BCS Code of Conduct, 4.7. 'Impartiality'.

Suggestion: Changes as already mentioned.

2.1. High Performance Standards

Why the restriction to 'Multinational' Organizations?

Suggestion: The word 'Multinational' should be omitted.

2.2. International Standards and Regulations

This is no more than an optimistic statement, but does not imply any moral demand.

Suggestion: This paragraph to be omitted.

2.3. International Legal Protection

The remarks made about 2.2. are also valid for 2.3.

Suggestion: This paragraph to be omitted.

2.4. Employee Productivity and Quality of Working life

Improvement of information systems doesn't necessarily mean an enhancement of the quality of working life for the employee. Apart from this the recommendations laid down in this paragraph show no specific bearing on the computerized workplaces or on data processing. Finally it is a matter of the national legislation in many countries to regulate management/labour relations.

Suggestion: This paragraph to be omitted.

---

[1] Apparently, reference is given to the 1984 Code of Conduct and not to the last 1992 version (see in this book); but 'professional integrity' is there treated in 4.3 and not in 2.2. Further reference to 'impartiality' in 4.7 is correct. *Note of the Editor.*

2.5. User Participation and Feedback

There is no doubt that the user must be seen as an integral part of the total information system. But the achievement of this desirable situation is far more a technical, organizational and economic matter than an ethical one. Involving the user raises also the question of the proper addressees of a Code of Ethics, a question which will be dealt with later on.

Suggestion: This paragraph to be omitted.

3.1. Intellectual Property Law

No comments.

3.2. International Public Law

This paragraph contains some statements which are undoubtedly correct but pertain to various laws and regulations whose scope goes far beyond the draft Code of Ethics in consideration.

Suggestion: This paragraph to be omitted.

3.3. International Telecommunication Law

Same remark as in 3.2.

Suggestion: This paragraph to be omitted.

3.4. International Criminal Law

The reference made to this novel crime, the computer crime, is indeed a very important one. But why the restriction to transnational computer crime, to international criminal use of computers? Similar crimes happen on a national level as well. Here again the question of the proper addressees for the Code of Ethics can be raised.

Suggestion: To change this paragraph in such a way as to replenish the remarks concerning international crime by a sentence referring to a general responsibility to fight computer crime also on a national and corporate level.

Paragraphs 3.1. - 3.4. contain recommendations and demands which presuppose lawgiving actions in order to be effective. These recommendations and demands partly overlap on already existing laws and regulations and they partly exhibit gaps in existing legislation: In any case they cannot act as guidelines for moral behaviour. They must be seen as demands to be addressed to a national and/or international legislature.

Suggestion: To comprehend the important content of these paragraphs, an epilogue to the Code of Ethics should be added.

4.1. Freedom of Communication

Suggestion: A reference to already existing legal protection of privacy should be added.

4.2. Privacy and Dignity of Individuals

Same remark and suggestion as in 4.1.

4.3. Humanized Information Systems

Suggestion: A reference to already existing health protection and working condition regulations should be added.

4.4. International Computer Literacy

No comments.

4.5. Equitable Opportunity for Information Service

The subject mentioned here is far beyond the scope of this draft Code of Ethics.

Suggestion: To express the ideas contained in this paragraph in an epilogue to the Code of Ethics.

4.6. Cultural Quality of Life and Human Choice

Same remark and suggestion as in 4.5.

Finally let us add some topics which we feel are missing in the present draft and which should be added in an appropriate way.

A. The draft refers to Information Technology (IT). This term refers strictly speaking to telephone, radio, television etc. as well, whereas the draft is meant for the 'computer world' only. As a matter of fact, the wording of the various paragraphs shows this more restricted meaning: We suggest therefore to replace IT by 'Computer Based Systems', 'Electronic Data Processing' or some such phrases.

B. Throughout the whole draft it is not clear who the addressees are, since no definition of the addressees is given. We consider this a crucial point. Many annotations to the single paragraphs come from this lack of clarity. We admit that this is an extremely difficult problem. Members of the profession of doctors or lawyers, for example, can be defined by their common educational background and their admission to certain activities. A person working in the 'computer world' however still has a vague position in society and evades any clear definition regarding educational background as well as the right for certain activities.

An Engineer's Hippocratic Oath[1]

I solemnly pledge myself to consecrate my life to the service of humanity. I will give to my teachers the respect and gratitude which is their due; I will be loyal to the profession of engineering and just and generous to its members; I will lead my life and practice my profession in uprightness and honor; whatever project I shall undertake, it shall be for the good of mankind to the utmost of my power; I will keep far away from wrong, from corruption, and from tempting others to vicious practice; I will exercise my profession solely for the benefit of humanity and perform no act for a criminal purpose, even if solicited, far less suggest it; I will speak out against evil and unjust practice wheresoever I encounter it; I will not permit considerations of religion, nationality, race, party politics, or social standing to intervene between my duty and my work; even under threat, I will not use my professional knowledge contrary to the laws of humanity; I will endeavour to avoid waste and the consumption of non-renewable resources. I make these promises solemnly, freely, and upon my honor.

---

[1] In: Ch. SUSSKIND, *Understanding Technology*, Baltimore and London: The John Hopkins University Press, 1973, p. 118.

Oath of an Informatician

Daniel LOEFFLER
Student in Informatics
University of Hamburg, Germany

(1993)

On the dignity of my humanity, I freely engage myself to fulfil this oath by my best knowledge and conscience:

I want to live and work honestly and sincerely and always do my best to follow my vocation (in the sense of this oath).

I am aware of my responsibility as a computer expert to process and safeguard all information in a correct way. I will work in an ecological consciousness of information to prevent the 'information-sphere' from pollution by faulty programs and wrong data.

I will act in a holistic and interdisciplinary way. I will be cautious not to separate subject and object, environment and interior system, or developers, users and usees, as all consequences of my actions in turn affect myself. I take responsibility for myself, for my thinking, feeling, speaking and acting, and I will only promise what I can keep.

I do not serve any egoistic interests, I will not allow misuse of information technics nor falsification of information, and I will give nobody the possibility to influence me adversely.

I will not use power to control others, and I shall not develop or distribute any destructive software. I will make public any unjust practice and any problem. I will do my best to find reasons of my own faults, and I will forgive others and correct mistakes. I will be open for suggestions and any constructive criticism.

I respect the human rights, the privacy of individuals and the democratic freedom of information. I accept myself and all human beings as they are, regardless of sex, religion, nationality and birth. I will stand up for keeping nature alive.

I respect my teachers and continue their work, in an evolutionary sense. I will work to increasing my knowledge and to a further global development.

If I follow this oath, I am allowed to do all things successfully, otherwise I disqualify myself.