23

Privacy at risk in the global information society

Simone Fischer-Hübner
Faculty for Informatics, University of Hamburg
Vogt-Koelln-Str. 30, D-22527 Hamburg-Stellingen
Tel: +49 40 5494 2225; Fax: +49 40 5494 2226
Email: fischer@rz.informatik.uni-hamburg.d400.de

Abstract

Privacy is a fundamental civil right which has to be protected in a democratic society. In the global information society, individual privacy is seriously endangered. An increasing amount of personal data is being transferred around the world and communication data of users could be easily traced and used to create individual communication profiles. International privacy regulations, besides the European Union Directive on Data Protection, will be needed because the communication using the new information infrastructure will be global.

This paper discusses privacy risks in the global information society. It also compares the Bangemann report and action plan with other national information infrastructure programmes (of the United States, Singapore, Japan, Canada, and Denmark) and critically analyzes their different approaches to privacy protection. The difficulties for a common harmonized approach to privacy protection, due to cultural differences, are shown. Moreover, privacy enhancing technologies are discussed. Finally, minimal requirements for a socially and privacy acceptable design and use of the information infrastructure are suggested.

INTRODUCTION

In the United States (US), the Clinton government started the National Information Infrastructure (NII) Programme (Clinton, 1993) for the further development of information highways to strengthen US communication and information technology. European politicians and industrialists did not want to miss out on opportunities for participation in the new information technology (IT) market and did not want to be put at a competitive disadvantage. A group of representatives,

An Ethical Global Information Society J. Berleur & D. Whitehouse (Eds.)

mainly from industry, under the chair of the vice-president of the European Union (EU) commission, Martin Bangemann, therefore elaborated a report and an action plan for the EU (Bangemann, 1994) to carry Europe forward into the global information society. In addition, many other nations (such as Canada, the Scandinavian countries, the Netherlands, Singapore, and Japan) meanwhile developed their own strategies. The Bangemann report and most other information infrastructure programmes promote initiatives such as teleworking, distance teaching, research networks, telematic services for enterprises, road and air traffic management systems, health care networks, public administration networks, and network access for all households through applications such as telebanking and video on demand. The programmes are mainly motivated by economic interests. They generate new jobs and economic growth, and provide better chances for people constrained by geography or disability. Furthermore, they help to overcome structural problems such as in traffic or in health care. On the other hand, the new information infrastructure will change our lives completely, and it bears different risks for society (CPSR, 1993; Fischer-Hübner and Schier., 1996). Individual privacy will be especially endangered, as more and more sensitive personal data can be quickly transferred around the world. Moreover, an increasing amount of transactional data for network services will be available and can be collected at different sites around the world. These data can be used to generate consumer and communication profiles. Privacy as a fundamental civil right (in Germany, a constitutional right) has to be protected in a democratic society. An international harmonization of privacy legislation, besides the EU Directive on data protection, is needed because in the global information society privacy is becoming more and more of an international problem.

This paper discusses privacy risks in the global information society. It shows that, due to cultural differences, there are significant deviations in the EU approach to privacy protection from the privacy regulations of other countries which have developed information infrastructure programmes. These different approaches to privacy protection are critically analyzed. Furthermore, privacy enhancing technologies are discussed, because they can be used technically to enforce legal privacy requirements. Finally, minimal requirements for a socially and privacy acceptable design and use of information highways are suggested.

PRIVACY

An often used definition of privacy is the one by Alan Westin: 'Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others' (Westin, 1967).

In general, the concept of privacy has three aspects (Rosenberg, 1992; Holvast, 1993):

- *territorial privacy* (by protecting the close physical area surrounding a person);
- *privacy of the person* (by protecting a person against undue interferences, such as physical searches or information violating his/her moral sense); and
- *informational privacy* (by controlling whether and how personal data can be gathered, stored or selectively disseminated).

Data protection is the protection of personal data in order to guarantee privacy and is only a part of the concept of privacy.

The emphasis of this paper is on the discussion of informational privacy of individuals. Individual informational privacy has also been defined by the German Constitutional Court in its Census Decision of 1983 as the term *right of informational self-determination*, meaning the right of an individual to determine the disclosure and use of his/her personal data on principle at her/his discretion.

In order to protect this right, privacy laws of many western states as well as the EU Directive on data protection (EU Directive, 1995) require basic privacy principles to be guaranteed when personal data are collected or processed. These include:

- purpose binding (personal data obtained for one purpose should not be used for another purpose without informed consent);
- necessity of data collection and processing (the collection and processing of personal data shall only be allowed, if it is necessary for the tasks falling within the responsibility of the data processing agency);
- the data subject's right to information and the right to correction, erasure or blocking of incorrect or illegally stored data;
- control by an independent data protection authority (also called supervisory authority, data protection commissioner, or ombudsman); and
- requirement of adequate technical and organizational security mechanisms to guarantee the confidentiality, integrity, and availability of personal data.

THREATS TO PRIVACY IN THE GLOBAL NETWORKED SOCIETY

In the global information society, privacy is seriously endangered. A key problem is that the traffic on a global network (for example on the Internet) crosses international boundaries and is not centrally managed. On the Internet, there is no overall responsibility assigned to a certain entity, and there is no international oversight mechanism to enforce legal obligations (especially data protection legislation), as far as they exist (Budapest Draft, 1996).

There are severe privacy risks, because personal data about the users or other data subjects are available and can be intercepted or traced at different sites around the world. Major risks are:

Transmission of great quantities of personal data

Meanwhile, the global information society is evolving rapidly and many new information highways for the health sector, public administration, research and private life are being developed. There is a growing amount of personal data, such as sensitive medical data, business data and private data that are accessible and are communicated through networks across state borders. Sensitive personal data can easily be communicated to or routed via countries without an appropriate privacy level. Messages transmitted in plain text could be intercepted or modified. Especially, the secret services are interested in controlling message content.

Communication and consumer profiles

A side-effect of global communication is that connection data are available at different sites around the world revealing details about communication partners, time of communication, services used, connections, and so on. These transactional data may reveal who communicated with whom, when, for how long, and who bought what for what price. Users leave an electronic trace which can be used to create consumer or communication profiles.

Every electronic message contains a header with information about the sender and recipient, as well as the routing and subject of the message. This information could be intercepted at each site passed. There is normally no anonymity of communication, because the recipient of an electronic mail (even if the email is encrypted) can determine the sender's identity through the sender's email address which normally contains information about the user's name, background (for example, university or company), and location.

Communication profiles could be created by the service provider to whom the user is connected (like Internet or mailbox providers). Service providers are recording personal user data (such as user name, login name, address, bank connection, and status) as well as accounting data for billing purposes. Users are normally identified and authenticated by the service providers, and their communication behaviour (for example, access to news or world wide web (WWW) sites could be easily traced and supervised by the providers.

Also, personal user data could be recorded at remote servers. A WWW server can only record the Internet Protocol (IP) addresses of requesting users, which normally do not reveal the user's identity. But techniques, such as Netscape's so-called cookies, could be used by the remote WWW servers to monitor the user's accesses to web pages. Cookies are variables that a server provider can store and later retrieve from the local WWW browser of the user. If a user is identified by the server as having ordered goods or registered for software, the cookies of this user revealing his/her interests in particular web pages can be related to his/her name or email address by the server.

There are several possibilities for the (mis)use of such communication profiles. For example, marketing agencies have a special interest in communication profiles, which can be used to send advertisements to consumers addressing their specific needs or interests. Also, the secret services are interested in information about users' access to newsgroups or WWW pages so as to have the ability to monitor the communication behaviour of individuals under suspicion.

Network insecurity

Another problem of the global information society is whether the requirements of appropriate technical and organizational security mechanisms to protect the personal data on the information highways and to provide network reliability can be guaranteed sufficiently. The Internet, an important contemporary information highway that consists of several thousand computer networks with several million users, is known for a lot of critical security holes. Accidents, such as the Internet worm, chain letter attacks, hacking attacks (such as the KGB hacking incident),

sniffer-password attacks, IP address spoofing, and malicious agents have demonstrated the insecurity of Internet technology.

Major reasons for Internet security problems are the lack of standardized cryptographic authentication, buggy host software, and the difficulties in system administration. There is no overall responsibility for security on the Internet; each site is responsible for its own security. The specification of the new improved IP version 6 is offering support for end-to-end encryption and authentication mechanisms in its protocol definition. However, encryption and authentication mechanisms can only be used in a secure manner with an infrastructure for key distribution which is not part of the specification.

Since security was not a main issue when the Internet was initially designed, it is now virtually impossible to fix many security holes.

In conclusion, in the global information society, privacy is at risk and is becoming more and more an international problem. Consequently, internationally harmonized privacy regulations are needed for an adequate level of privacy protection. Furthermore, data protection commissioners demand that privacy protection should be technically enforced and should already be integrated in the system design.

PROBLEMS OF AN INTERNATIONAL HARMONIZATION OF PRIVACY LEGISLATION

In the Bangemann report it is written:

> '...Without the legal security of a Union-wide approach, lack of consumer confidence will certainly undermine the rapid development of the information society. Given the importance and sensitivity of the privacy issue, a fast decision from Member States is required on the Commission's proposed Directive setting out general principles of data protection.'

In the EU, privacy protection will be enforced by *the EU Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (EU Directive, 1995). The EU Directive was formally adopted in 1995 by the European Council. It has to be used by member states to amend their respective national laws (where necessary) to comply with the requirements of the directive by 1998. Besides the privacy protection of individuals, another objective of the EU Directive is to require a uniform minimum standard of privacy protection to prevent restrictions on free flow of personal data between EU member states for reasons of privacy protection.

Even if the EU Directive can help to enforce a relatively high standard of data protection in Europe, it will not be able to protect privacy sufficiently in the global information society. As discussed above, personal data can easily be transferred or routed across state boundaries to countries without any data protection legislation, where its information content or communication data can be intercepted. Privacy is therefore an international problem, and an international harmonization of privacy regulations is needed.

The critical question remains whether a common harmonized approach to privacy will be possible due to cultural, historical, and political differences. Anthropologists have stated that, on a low level, privacy (especially privacy of the

person and of the close surroundings) is a human physiological need. But, on higher organizational levels, privacy is basically a cultural construct and there are considerable cultural variations in privacy needs and interests (Lundheim and Sindre, 1994). In addition, experiences from World War II, especially the practice of the Nazi government in amassing and misusing great amounts of personal details about the population, have caused a greater sensitivity to privacy in western European states (Madsen, 1992). Another problem can be seen in non-democratic societies, where individual privacy is normally not protected by legislation. On the contrary, in these countries privacy is often invaded by the state.

In the following sections, the privacy approaches of technologically developed states that have set up information infrastructure programmes are compared with the EU approach. Thereby, considerable distinctions in the different national approaches to privacy protection are shown. Furthermore, all the approaches are critically analyzed to determine the insufficiencies of privacy legislations.

European Union

According to the Bangemann report, the EU Directive will provide protection of privacy through the member states in the global information society.

The EU Directive makes no differentiation between rules applied in the public and in the private sector. The EU Directive is focused on personal data protection. It sets out general rules on the lawfulness of data processing which should also enforce the basic privacy principles mentioned in the earlier part of this article on privacy. It could be used to enforce a relatively good level of data protection in Europe. However, it has also been criticized that some rules (especially the criteria for making data processing legitimate - Article 7) are very general and allow a variety of specific implementations in national laws. These differences in interpretation could hinder the goal of reducing divergences between national laws.

The EU Directive also contains provisions for the transfer of personal data to third countries outside the EU. According to Article 25, the export of personal data to third countries, which do not provide an adequate level of protection, is prohibited. However, in open and free networks, such as the Internet, with no central agency of control, it is technically difficult to enforce this requirement (Koch, 1995).

It has also been criticized that many rules of the EU Directive include exceptions that are mandatory and may hinder states in providing a stricter standard of privacy protection (Greenleaf, 1995).

Singapore

The information infrastructure plan *IT2000 - A Vision Of An Intelligent Island* was formulated by the Singapore government in August 1991 (Singapore, 1991). By 2000, Singapore, the Intelligent Island, should be among the first countries with an advanced information infrastructure that will link government, business, and people. Singapore, like most other Asian states, does not have any privacy protection laws so far. On the contrary, privacy does not seem to be a topic at all. Intensive surveillance by security services is justified by Singapore's Internal Security Act. While promoting the use of the SINGNET (Singapore's Internet

sub-network), the government is trying to control the content of the information transmitted over the net at the same time (Madsen, 1995).

Japan

In June 1993, the Information Industry Committee of the Industrial Council in Japan issued a report stating the need for the government to promote information technology. In May 1994, the Ministry of International Trade and Industry (MITI) published a *Programme for Advanced Information Infrastructure*. In this programme under the topic *Improvement of Environment for Realizing Advanced Information Society*, only security measures, and not privacy issues, are discussed (Japan, 1994).

Japan, on the other hand, is one of the very few Asian countries to have implemented a data protection act. The awareness of privacy in Japan has resulted more from economic self-interest than from any longstanding tradition of ensuring individual privacy (Madsen, 1992). The Japanese *Act for Protection of Computer Processed Personal Data* was made official in December 1988. In addition, cities, towns, and villages have also enacted local privacy regulations. However, the Japanese data protection act only applies to national government organizations. Moreover, it does not install an independent data protection authority to control data processing. In 1989, MITI issued formal guidelines entitled *Protection of Personal Data Processed by Computers in the Private Sector*. However, these guidelines for privacy in the private sector are not mandatory and can only be adopted internally by private companies.

United States of America

In 1993, the Clinton/Gore government presented the *National Information Infrastructure (NII) Programme - Agenda for Action* (Clinton, 1993). So far, the US has been criticized for being the first in technology but the last in data protection (Madsen, 1992). The US Privacy Act of 1974 only covers the public sector. Besides the Privacy Act, there is only a non-uniform patchwork of various privacy and computer security legislation. The US does not have a data protection authority to oversee privacy protection and to act if there are complaints from data subjects about unfair or illegal use of their personal data. Consequently, the only way for data subjects to fight against data misuse is through the courts.

It has been realized that the NII does not only promise many benefits, but is also increasing risks to privacy. Therefore, the Information Infrastructure Task Forces (IITF) Working Group on Privacy has developed privacy principles with the goal of providing guidance to all participants in the National Information Infrastructure (IITF, 1995). They are intended to be applied to governmental and private sectors, and are based on the idea that all participants (information providers, collectors, users, and data subjects) of the NII have a shared responsibility for the proper use of personal information..

General Principles for All Participants require that all NII participants should ensure and respect information privacy, information integrity, and information quality.

Privacy approaches in selected information infrastructure programmes

Information Infrastructure Programmes	Privacy regulations	Criticisms to privacy approaches
Singapore *IT2000 - Vision of an Intelligent Island, 1991*	--	- Internal Security Act allows intensive surveillance - attempts to control information content transmitted over the net
Japan *Programme for Advanced Information Infrastructure* Report by *Information Industry Committee of Industrial Structure Council,* 1993	Japan Data Protection Act (1988) MITI Guideline *Protection of Personal Data Processed by Computers in the Private Sector* (1989)	- applicability to public sector only - no data protection authority - not mandatory
USA *National Information Infrastructure (NII) Programme*, 1993	US Privacy Act (1974) + Privacy Acts of states IITF-WG on Privacy - Privacy Principles (1995)	- applicability to public sector only - no data protection authority - not mandatory - shared responsibility of data protection agency/usees will not work - no control of independent data protection authority
Canada *The Canadian Information Highway,* discussion paper: 1994 Final report by *Information Highway Advisory Council,* 1995	Canada Privacy Act (1982) + Privacy Acts of Quebec and Ontario CSA *Model Code for Protection of Personal Information* (1996)	- applicability to public sector only (except Quebec) - no legislation so far
EU *Europe and the Global Information Society,* (Bangemann Report), 1994	EU Data Protection Directive (1995)	- too general, too many exceptions - art. 25 can hardly be enforced on the Internet
Denmark *Info-Society 2000,* 1994	The Danish Private and the Danish Public Authorities Register Acts (1978) *Utilisation of Data and Protection of Personal Data*	- applicability to registers only - multifunctional use of data, not purpose binding

Principles for Users of Personal Information require information users to assess the impact on privacy of current or planned activities and to use personal information only for these activities or for compatible uses. Data subjects will be informed by the data collector about the reason and purpose of data collection and about their rights. Information users should use appropriate security mechanisms to protect the confidentiality and integrity of personal data. Information users should not use information in ways that are incompatible with an individual's understanding. Furthermore, they should educate themselves about how privacy can be maintained.

According to the *Principles for Individuals Who Provide Personal Information*, individuals should obtain information about what data is being collected and for what reason, and how it will be protected. Individuals will have a responsibility to understand the consequences of providing personal data to others and will make intelligent choices on whether to provide or not to provide their personal data. Individuals will be able to safeguard their own privacy by having the means to obtain their data, to correct them, to use appropriate technical safeguards (for example, encryption), and to remain anonymous when appropriate. Furthermore, data subjects will have means of redress, if harmed by an improper disclosure or use of personal data.

The IITF privacy principles could raise the level of data protection in the US, especially if applied in the private sector. Unfortunately, the principles only offer guidelines for those who are drafting laws and regulations but they do not have the force of law. Although the IITF privacy principles are intended to be consistent with international guidelines such as the Organization for Economic Cooperation and Development guidelines, they do not in some respect offer the same level of privacy protection as the EU directive. In practice, the idea of shared responsibility of equal partners will not always work, because data subjects (such as employees) often depend on services provided by the data processing agencies (for example, employers), so that they hardly have the chance to enforce their rights themselves. Consequently, besides the right of redress, the control of an independent data protection authority is necessary to protect data subjects efficiently.

Canada

In September 1995, the Canadian Information Highway Advisory Council presented the final report *Connection Community Content: The Challenge of the Information Highway* (Canada, 1995). In contrast to most other information infrastructure programmes, which were mainly influenced by input from representatives of the IT industry, the advisory council also included members from artistic, creative, and educational communities, and from consumer and labour organizations. It was chaired by David Johnston, professor of law at McGill University's Centre for Medicine, Ethics and Law.

The Canadian Privacy Act of 1982 which, in contrast to the US legislation, established the Office of Privacy Commissioner, only applies to federal government bodies and agencies. Only the province of Quebec has enacted specific legislation for the private sector. In order to overcome these deficiencies in the private sector, the Canadian Standard Association (CSA) is developing a model of a voluntary privacy code for use by the private sector.

Privacy protection and network security were one of five principles that were set up by the Information Highway Advisory Council. The council recommends that the government should continue to collaborate with the CSA, business, and consumer organizations, and other levels of government in order to implement the CSA draft code and develop effective independent oversight and enforcement mechanisms.

Denmark

The Danish approach is discussed to show that, even in the European Union, there is not a complete consensus on the approach of the EU Directive on data protection. The Danish Private Register Act as well as the Danish Public Authorities Registers Act of 1978 protect personal data in registers and cannot be applied to other form of personal data (for example, personal data included in electronic mail). For this and for other reasons, it is regarded as outdated and its amendment is planned.

The Danish proposal *Info-Society 2000* (DMR, 1994) was worked out by a two-member committee appointed by the government and was published in 1994 by the Danish Ministry of Research. Statements to the parliament on *Info-Society 2000* and action plans for the initiatives for the coming years were presented by the government in 1995 and in 1996.

In the *Info-Society 2000* proposal, the EU directive was criticized for being too bureaucratic. Modern legislation that makes it possible to register, combine, and use data for all legal and administrative purposes without bureaucratic procedures, was demanded. According to the report, it should be possible to collect and register non-sensitive information and to use it more or less freely, as well as to transfer it, provided that due respect is paid to the principle of transparency. The principle of transparency should, on the other hand, not be administered rigidly or inflexibly. However, the Danish public also commented critically that the free use of personal data for different purposes can endanger personal privacy. The more or less free use of personal data is actually an infringement of the internationally accepted privacy principle of purpose binding. It is not considered that there are no non-sensitive data. Also, personal data such as addresses that seem to be non-sensitive *per se*, can become highly sensitive if used for a specific purpose in a certain context. The Danish proposal gives an example of how changes to privacy legislation are discussed, not because individuals will be protected from increasing privacy risks but rather because free communication on the information highways will be legalized.

PRIVACY ENHANCING TECHNOLOGIES

In a fully networked society, privacy is seriously endangered and cannot be sufficiently protected by privacy legislation alone. Data protection commissioners are therefore demanding that privacy requirements should also be technically enforced and that privacy should be a design criterion for information systems. The Dutch Data Protection Authority (the Registratiekamer) and the Information and

Privacy Commissioner (IPC) for the Province of Ontario, Canada, have collaborated in the production of a report (Registratiekamer/IPC, 1995) exploring privacy enhancing technologies that safeguard personal privacy by minimizing or eliminating the collection of identifiable data.

The report on privacy enhancing technologies by the Registratiekamer and IPC, and a prior study of the Registratiekamer on how to design and model privacy technologies, (Registratiekamer, 1995) mainly focus on privacy technologies that permit transactions to be conducted anonymously. Extended security criteria for systems with high privacy requirements should cover a diversity of privacy enhancing security aspects such as:

- *Anonymity, Pseudonymity, Unlinkability, Unobservability of users:* The privacy principle of necessity of data collecting means that personal data should not be collected or used for identification purposes when not really necessary. Consequently, information systems should guarantee that, if possible, users can act anonymously.
- *Anonymity and Pseudonymity of data subjects:* If storage is needed, personal data of data subjects should be anonymized or pseudonymized as soon as possible.
- *Purpose binding and necessity of data processing of personal data of users and data subjects:* If personal data have to be processed, the privacy principles of purpose binding and necessity of data processing can be technically supported through an appropriate security policy and access control mechanisms (for example, see Fischer-Hübner, 1994, for a formal privacy enforcing access control model).

In the global information society, privacy technologies that provide anonymity or pseudonymity for the users will be needed to prevent the creation of communication and consumer profiles. So far, there are only a few privacy technologies available for protecting user identities. Examples are:

- *Prepaid cards* (e.g., telephone cards) for charging services;
- David Chaum's *DigiCash* which is based on blind signatures. It can be used as an electronic form of anonymous payment that can be transmitted over the networks (see Chaum, 1985; Chaum, 1990). DigiCash's Ecash has been tested for several years and was used in 1995 to issue the first ecash dollars in the US. Also, an Australian bank will soon use DigiCash to issue ecash, and a big German bank and Digicash's Ecash are to launch a joint pilot project to test the use of electronic cash on the Internet.
- *Anonymous remailers* provide a free service that allows email to be sent without the recipient knowing who sent the message. The message is sent through an intermediary computer which secretly passes the message to the recipient. Anonymous remailers cannot completely guarantee email privacy. A mapping of anonymous identities to real addresses must be maintained by the remailer which, for that reason, can be a sensitive point of attack. There was an earlier incident in which the Finnish police, in cooperation of the Federal Bureau of Investigation (FBI) raided the residence of a Finnish provider of an anonymous remailer. The FBI is opposed to anonymous remailer services but formally acted on a complaint from the Church of Scientology about stolen scientology files posted on the remailer. Such incidents could probably easily happen again. Besides, unscrupulous providers could monitor the traffic that

goes through the remailers. In any case, the user has to place a high degree of trust in the anonymous remailer. For sensitive communication, encrypted messages should be sent through several remailers.

The report of the Registratiekamer and IPC (Registratiekamer/IPC, 1995) concludes that, if privacy technologies are to play a more significant role, it will be necessary to create more public awareness as well as consumer demand for them. If there is a demand, providers will probably try to respond to market forces.

Security mechanisms, such as access control or encryption, are necessary to protect the confidentiality and integrity of personal data, if personal data have to be processed/transmitted. Such security mechanisms can be better classified as data protection technologies (in contrast to privacy enhancing technologies).

The Bangemann report emphasizes the importance of encryption to protect personal data but also claims that governments may need powers to override encryption for the purposes of fighting against crime and protecting national security. In France, the free use of encryption is already restricted by law. Legal forms of the regulation of encryption are also being discussed in other European states and by the European Commission. However, as the cryptographic policy debate demonstrated, such regulations of encryption will primarily endanger the possibilities of individuals to communicate freely and to protect their own personal data. Criminals or terrorists will still find ways to hide secret messages (for example, through steganography) without being detected.

MINIMAL REQUIREMENTS FOR A SOCIALLY AND PRIVACY ACCEPTABLE DESIGN AND USE OF THE INFORMATION INFRASTRUCTURE

Only leading representatives from industry were initially invited to contribute to the Bangemann report. Consequently, economic opportunities were emphasized while social impacts were neglected. Most other information infrastructure programmes were also mainly motivated by economic interests.

For a socially acceptable design of the global information society and for a democratic proceeding, the public should be fully involved in policy-making. Representatives from public interest communities (usee organizations) and social and legal scientists, who can assess and consider the social and legal impacts adequately, especially should participate in the design of the information society. Some minimal requirements for a socially and privacy acceptable design and use of the information infrastructure are as follows (see also CPSR 1993; Fischer-Hübner and Schier, 1996):

- Democratic participation of the public in the design and development of the information infrastructure should be encouraged.
- Social and legal impacts of different initiatives should be assessed in advance in cooperation with representatives from usees' organizations and from public interest communities as well as in cooperation with social and legal scientists. Initiatives should be carefully tested in pilot projects for aspects of social acceptability. Initiatives with non-acceptable risks to privacy and/or society should not be implemented.

- Social impacts have to be considered and initiatives should be periodically reviewed to ensure that they continue to serve public interests.
- Internationally obligatory privacy regulations besides the EU directive are needed. These regulations should guarantee basic privacy principles for an adequate protection of privacy in the global information society.
- Security and privacy issues have to be considered from the beginning and should be integrated into the system design. Privacy enhancing technologies have to be implemented if possible.
- High security standards and network reliability should be required.
- Users should be permitted to use strong cryptography to protect communication.

These minimal requirements must be considered, and enforced, from the beginning and throughout the design of the information society.

REFERENCES

(Bangemann, 1994) Europe and the global information society, Recommendations to the European Council, Brussels, 26 May 1994 (Bangemann report), http://www.earn.net/EC/bangemann.html

(Budapest Draft, 1996) International Working Group on Data Protection in Telecommunications, Data Protection on the Internet, Report and Guidance (Budapest Draft), May 1996.

(Canada, 1995) Connection Community Content: The Challenge of the Information Highway, Final Report of the Information Highway Advisory Council, September 1995.

(Chaum, 1985) D. Chaum, Security without Identification: Transaction Systems to Make Big Brother Obsolete, *Communications of the ACM*, **28** (10). 1985, pp.1030-1044.

(Chaum, 1990) D.Chaum, Achieving Electronic Privacy, *Scientific American*, August 1992, pp.76-81.

(Clinton, 1993) Clinton/Gore, The National Information Infrastructure: Agenda for Action, 1993.

(CPSR, 1993) Computer Professionals for Social Responsibilities: Serving the Community: A Public-Interest Vision of the Nation Information Infrastructure, *The CPSR Newsletter*, Winter 1994.

(DMR, 1994) Ministry of Research and Information Technology, Denmark, INFO-Society 2000, November 1994.

(EU Directive, 1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

(Fischer-Hübner, 1994) S. Fischer-Hübner, Towards a Privacy-Friendly Design and Use of IT-Security Mechanisms, *Proceedings of the 17th National Computer Security Conference*, Baltimore, October 1994.

(Fischer-Hübner, and Schier, 1996) S. Fischer-Hübner and K.Schier, Der Weg in die Informationsgesellschaft - Eine Gefahr fur den Datenschutz, in: Britta Schinzel (Ed.): *Schnittstellen*, Vieweg-Verlag, 1996 (in German).

(Greenleaf, 1995) G. Greenleaf, The 1995 EU Directive on Data Protection - An Overview, *The International Privacy Bulletin*, published by Privacy International, **3** (2), April-June 1995.

(Holvast, 1993) J. Holvast, Vulnerability and Privacy: Are We on the Way to a Risk-Free Society?, in: J.Berleur *et al.* (Ed.): *Facing the Challenge of Risk and Vulnerability in an Information Society*, Proceedings of the IFIP-WG9.2 Conference, Namur May 20-22, 1993, Elsevier Science Publishers B.V. (North-Holland), 1993.

(IITF, 1995) Information Infrastructure Task Force - Privacy Working Group: Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, Final Version, June 1995.

(Japan, 1994) Ministry of International Trade and Industry (MITI), Programme for Advanced Information Infrastructure, May 1994.

(Koch, 1995) F. Koch, European Data Protection - Against the Internet?, *Privacy International Conference on Advanced Surveillance Technologies*, Copenhagen, September 1995.

(Lundheim and Sindre, 1993) R. Lundheim and G. Sindre, Privacy and Computing: a Cultural Perspective, in: R. Sizer *et al.* (ed.): *Security and control of Information Technology in Society,* IFIP WG 9.6 Working Conference, St.Petersburg, 1993, Elsevier Science Publishers.

(Madsen, 1992) W. Madsen, *Handbook of Personal Data Protection*, Stockton Press, 1992.

(Madsen, 1995) W. Madsen, Securing Access and Privacy on the Internet, in: *Proceedings of the COMPSEC-Conference*, London, October 1995, Elsevier Science Publishers.

(Registratiekamer, 1995) Registratiekamer, Privacy-Enhancing Technologies: The Path to Anonymity, Volume II, Achtergrondstudies en Verkenningen 5B, Rijswijk, August 1995.

(Registratiekamer/IP, 1995) Registratiekamer, the Netherlands and Information and Privacy Commissioner/ Ontario, Canada, Privacy-Enhancing Technologies: The Path to Anonymity, Volume I, Achtergrondstudies en Verkenningen 5A, August 1995.

(Rosenberg, 1992) R. Rosenberg, *The Social Impact of Computers*, Academic Press, 1992.

(Singapore, 1991) National Computer Board (NCB)/ Singapore, IT2000 - A Vision of an Intelligent Island, August 1991.

(Westin, 1967] A. Westin, *Privacy and Freedom*, New York, 1967.